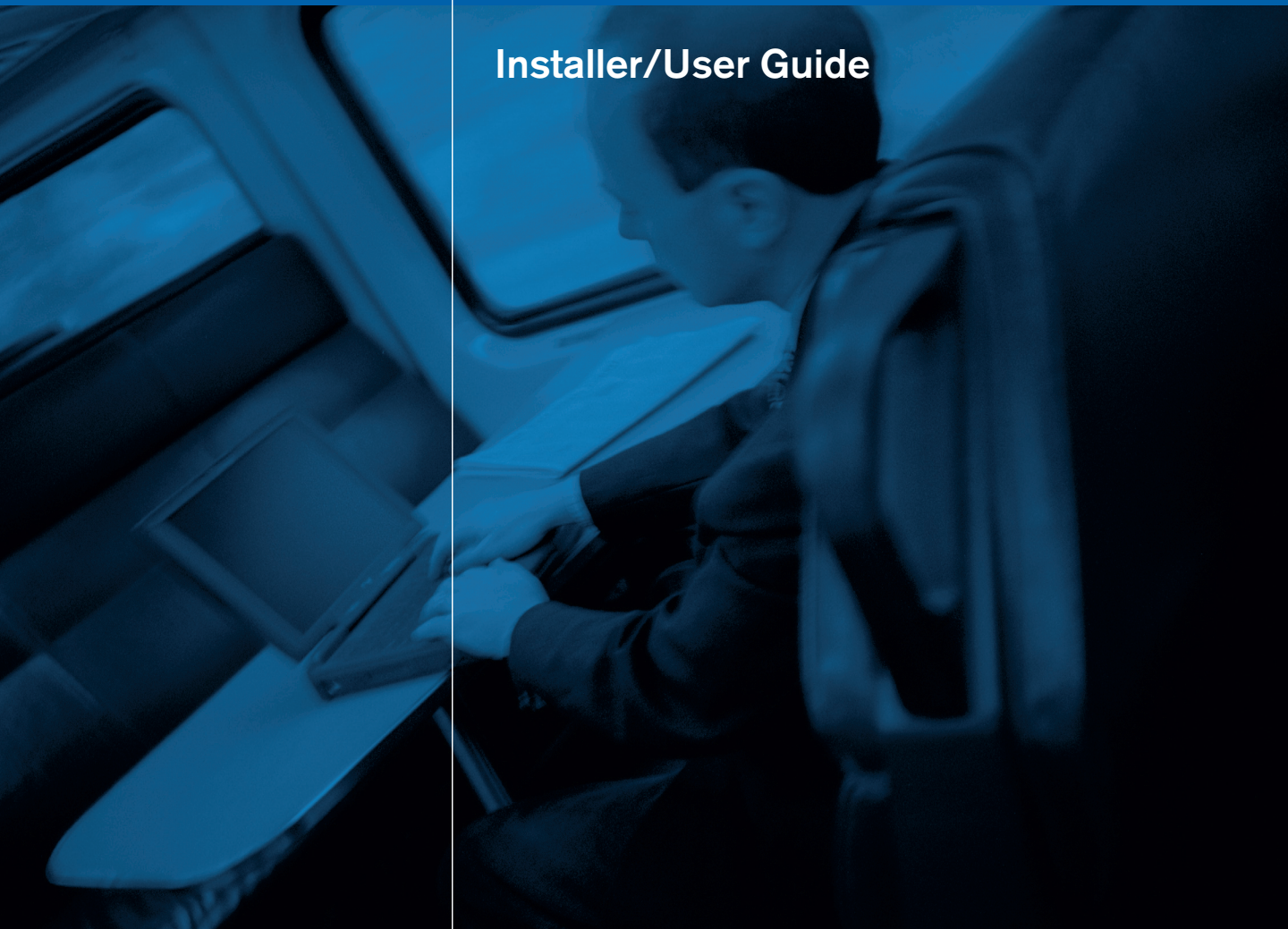
Avocent

DSView®

Installer/User Guide





INSTRUCTIONS

This symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.



DANGEROUS VOLTAGE

This symbol is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.



POWER ON

This symbol indicates the principal on/off switch is in the on position.



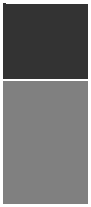
POWER OFF

This symbol indicates the principal on/off switch is in the off position.



PROTECTIVE GROUNDING TERMINAL

This symbol indicates a terminal which must be connected to earth ground prior to making any other connections to the equipment.



DSView®

Management Software Installer/User Guide

Avocent, the Avocent logo, The Power of Being There, DSView, DSR, AutoView, OutLook, OSCAR, AVWorks and Dambrackas Video Compression are trademarks or registered trademarks of Avocent Corporation or its affiliates. All other marks are the property of their respective owners.

© 2005 Avocent Corporation. All rights reserved. 590-395-501D

TABLE OF CONTENTS

List of Figures ..... **xi**

List of Tables ..... **xiii**

Chapter 1: Product Overview **1**

Features and Benefits *1*
System Components *2*
Supported Units *4*
About the DSView Explorer Windows *8*
Accessing target devices *9*
Using the side navigation bar *12*
Sorting information in a window *13*
Filtering information in a window *13*
Saving information in a window *15*
Using the Customize link in windows *15*
Displaying pages *16*
Bookmarking a window *17*
Printing a window *17*
Refreshing a window *17*
Using keyboard commands *17*
Profiles *19*
Changing user options *19*
Changing the color scheme *19*
Changing your password *20*
Enabling/disabling use of a third party Telnet application *20*
Specifying a user certificate *21*
Specifying an SSH key *22*
Built-in User Groups *22*
Preemption Levels *24*
Other Features and Considerations *25*
Configuring Internet Explorer *26*
Using certificates *31*
Using Integrated Windows Authentication *32*

Using the software through a firewall *32*
Using a VPN *33*
Using a NAT device *34*

Chapter 2: Installation 37

About Installation *37*
Installing the DSView Management Software *38*
Configuring the DSView Management Software *41*
Installing the DSR Remote Operations Software (Optional) *43*
Running the DSView Management Software *45*
Uninstalling the DSView Management Software *46*
Ending a DSView Software Session *47*
Java Installation *47*

Chapter 3: DSView Software Servers 49

Server Properties *49*
Certificates *51*
Proxy servers *53*
Server trap destinations *54*
Client session information *54*
Email *55*
Unit status polling *55*
Manually Backing up and Restoring Hub Servers *55*
Managing Authentication Services *58*
Managing Spoke Servers *73*
Replication *77*
Managing Licenses *79*

Chapter 4: Managing Units 81

About Unit Views *81*
Showing and hiding units *83*
Customizing Unit Views windows *84*
About Embedded Units *87*
Launching embedded unit sessions *88*
Adding Units *88*

Managing Units *95*
Changing Unit Overview Information *95*
Changing Embedded Unit Credentials *98*
Changing Unit Properties *99*
Changing Unit Access Rights *102*
Changing Managed Appliance Settings *106*
Managing and changing port settings *111*
Displaying and changing session settings on managed appliances *121*
Changing local account settings *127*
Managing Active Sessions *129*
Managing Connections to Units *132*
Connection display format *132*
Adding target device connections *134*
Unit Grouping *135*
Grouping units by site *135*
Grouping units by department *138*
Grouping units by location *140*
Grouping units by unit group *141*
Managing units by custom fields *144*
Chapter 5: Managing User Accounts 149
About the User Accounts Windows *149*
Customizing the User Accounts window *151*
Adding User Accounts *153*
Deleting User Accounts *155*
Unlocking User Accounts *155*
Resetting a User Account Password *155*
Changing User Account Properties *155*
Changing usernames *156*
Changing certificates associated with users *156*
Specifying a user SSH key *157*
Changing user passwords *157*
Specifying user account restrictions *158*
Changing user group membership *158*
Changing the preemption level for a user *159*

Specifying user address information *159*
Specifying user phone contact information *160*
Specifying email contact information for users *160*
Specifying user notes *160*
Changing custom field properties *161*
Displaying User Access Rights *161*
Managing User Groups *163*
Adding user-defined user groups *164*
Deleting user-defined user groups *166*
Displaying and changing user group properties *166*
Displaying and changing user group members *167*
Displaying user group unit access rights *168*

Chapter 6: Using the Video Viewer 171

About the Video Viewer Window *171*
Video Viewer minimum requirements *172*
Launching a KVM Session *172*
Launching an exclusive KVM session *173*
Connecting to an existing session *173*
Window Features *175*
Specifying Video Viewer Session Settings *177*
Changing the toolbar *177*
Toggling menu and toolbar activation *178*
Setting the Window Size *178*
Adjusting the View *179*
Using background refresh *180*
Adjusting color depth *181*
Additional Video Adjustment *181*
Adjusting Mouse Options *184*
Cursor Type *185*
Cursor settings *186*
Scaling *186*
Alignment *187*
Using Scan Mode *187*
Thumbnail Viewer features *188*

Performing Thumbnail Viewer tasks *190*
Using Keyboard Pass-through *191*
Using Global and Personal Macros *192*
Power Controlling Target Devices *199*
Displaying Video Viewer Users *199*
Saving the View *200*
Closing a Video Viewer Window Session *200*
Using Virtual Media *200*
Virtual Media dialog box *202*
Virtual media session settings *202*
Opening a virtual media session *203*
Closing a virtual media session *204*
Troubleshooting *205*

Chapter 7: Using the Telnet Viewer 207

About the Telnet Viewer *207*
Telnet Viewer Window Features *208*
Telnet Viewer window toolbar *209*
Security Property *210*
Opening a Session *210*
Customizing the Telnet Viewer *211*
Customizing Session Properties *212*
Login scripts *215*
Reviewing Session Data *216*
Macros *217*
Logging *221*
Log files *221*
Copying, Pasting and Printing Session Data *223*
Power Controlling Target Devices (Serial Session Only) *225*
Closing a Telnet Viewer Session *226*

Chapter 8: Working with IPMI 1.5 Target Devices 227

Adding and Changing DSI5100 Appliance BMCs *227*
Adding BMCs for use with a DSI5100 appliance *228*
Displaying Sensor Information Using the IPMI Viewer *230*
Launching an IPMI Viewer session *230*

IPMI Viewer Window features *230*
Refreshing the IPMI Viewer window *233*
Closing an IPMI Viewer window *233*
Displaying Sensor Information by Selecting an IPMI 1.5 Target Device *233*
Displaying IPMI 1.5 target device BMC information *234*
Displaying LAN configuration information *235*
Displaying field replaceable unit (FRU) information *235*
Displaying IPMI 1.5 target device discrete sensor information *236*
Displaying IPMI 1.5 target device numeric sensor information *237*
Displaying the BMC system log and log events *239*
Chapter 9: Using Tools 243
Using Unit Tools *243*
Exporting units *243*
Exporting unit rights *245*
Merging target devices *246*
Importing DSView 2.x software databases *247*
Using the Managed Appliance Tools *250*
Rebooting *251*
Upgrading firmware *252*
Resynchronizing managed appliances *252*
Saving a managed appliance configuration *253*
Restoring a managed appliance configuration *254*
Saving the user database of a managed appliance *254*
Restoring the user database of a managed appliance *255*
Managing Tasks *255*
Adding tasks *256*
Specifying when to run tasks *257*
Adding tasks using the Add Task Wizard *259*
Running tasks manually *270*
Displaying task results *270*
Deleting tasks *271*
Changing tasks *271*
Firmware Management *272*
Chapter 10: Event Logs 275

About Event Logs *275*
DSView management software events *277*
Displaying Event Logs *281*
Using the Date Filter *283*
Displaying the Details of Event Log Entries *284*
Deleting Event Log Entries *284*
Enabling and Disabling Events *284*
Retaining the Event Log *285*
Configuring Email Notifications *285*
Changing email notifications *287*
Deleting email notifications *287*
Testing email notifications *288*
Using the Event Log Tool *288*
Appendices **291**
Appendix A: Technical Support *291*
Appendix B: TCP and UDP Ports *292*
Appendix C: DSR Remote Operations Software *301*
Appendix D: Terminal Emulation *311*
Appendix E: Regaining Access to the DSView Software *327*
Appendix F: Glossary *328*
Index **339**

LIST OF FIGURES

Figure 1.1: Example System Configuration Using the DSView Management Software 7
Figure 1.2: Avocent DSView Explorer Window 8
Figure 1.3: Launching DSView Management Software Sessions 11
Figure 1.4: Side Navigation Bar 12
Figure 1.5: Typical DSView Software System Firewall Configuration 33
Figure 1.6: DSView Software System on a VPN 34
Figure 1.7: Single NAT Configuration (Client Only) 35
Figure 1.8: Double-NAT Configuration (Client and Corporate) 35
Figure 4.1: Shown and Hidden Units in a Recently Accessed Units Window 83
Figure 4.2: Alternate Actions Arrow in a Unit Views Window 86
Figure 4.3: Displaying Sites 136
Figure 4.4: Units in Custom Field Window 144
Figure 4.5: Custom Fields Example: Side Navigation Bar 147
Figure 5.1: User Accounts - All Window 150
Figure 6.1: Video Viewer Window (Normal Window Mode) 175
Figure 6.2: Manual Video Adjust Dialog Box 182
Figure 6.3: Video Viewer Window with Local and Remote Cursors Displayed 185
Figure 6.4: Thumbnail Viewer 189
Figure 7.1: Telnet Viewer Window 208
Figure 8.1: IPMI Viewer Window 231
Figure 8.2: Upper and Lower Threshold Values 233
Figure 8.3: Numeric Sensor Threshold Gauge 239
Figure B.1: Ports Used with a DS1800 Digital Switch or DSR Switch Connection (KVM) Without Proxy 293
Figure B.2: Ports Used with a DS1800 Digital Switch or DSR Switch Proxy Server Connection (KVM) 294
Figure B.3: Ports Used with a CPS or CCM Appliance Connection (Serial) Without Proxy 295
Figure B.4: Ports Used with a CPS or CCM Appliance Proxy Server Connection (Serial) 296
Figure B.5: Generic Appliance Session Ports 297
Figure B.6: External Authentication Server Ports 298
Figure B.7: Ports Used by SNMP (No External SNMP Manager) 298
Figure B.8: Ports Used by SNMP (with External SNMP Manager) 299

Figure B.9: Ports Used by DSI5100 Appliances *300*
Figure C.1: Using the DSR Remote Operations Software with a DSR Switch *302*
Figure C.2: DSR Remote Operations Window *303*
Figure C.3: DSR Remote Operations Window (Servers View) *304*
Figure C.4: DSR Remote Operations Window (Power View) *305*
Figure C.5: DSR Remote Operations Window (Versions View) *306*

LIST OF TABLES

Table 1.1: DSView Explorer Window Area Descriptions 8
Table 1.2: Managed Appliance Icons 9
Table 1.3: DSView Explorer Window Links 9
Table 1.4: Side Navigation Bar Icons 13
Table 1.5: Filter Field Text Strings 14
Table 1.6: DSView Explorer Page Navigation Buttons 16
Table 1.7: General Keyboard Commands 18
Table 1.8: Calendar Keyboard Commands 18
Table 1.9: Spinner Keyboard Commands 18
Table 1.10: Built-in User Groups and Allowed Operations 23
Table 1.11: User and User Group Preemption Levels 25
Table 3.1: Server Properties 49
Table 3.2: DSView Software Spoke Server Status Icons 74
Table 4.1: Unit Status Icons 85
Table 4.2: Actions to Initiate DSView Software Sessions 86
Table 4.3: CCM Appliance NFS Status Values 108
Table 4.4: Windows Containing a Site, Department or Location Column 136
Table 4.5: Links for Adding, Changing or Removing Site, Department or Location Association 138
Table 5.1: User Status Icons 151
Table 6.1: Video Viewer Window Descriptions 176
Table 6.2: Manual Video Adjust Dialog Box Descriptions 183
Table 6.3: Thumbnail Viewer Descriptions 189
Table 6.4: Virtual Media Session Settings 202
Table 7.1: Telnet Viewer Window Descriptions 208
Table 7.2: Telnet Viewer Window Toolbar Icons 209

Table 7.3: Arrow Key Sequences *213*
Table 7.4: Terminal Emulation and Type *214*
Table 8.1: IPMI Viewer Window Descriptions *231*
Table 8.2: IPMI Viewer Window Status Icons *232*
Table 8.3: Upper and Lower Threshold Gauge Colors *232*
Table 8.4: Numeric Sensor Threshold Icons *238*
Table 9.1: Task Status Icons *256*
Table 10.1: Event Log Severity Icons *276*
Table 10.2: Appliance Events *277*
Table 10.3: System Events *278*
Table 10.4: Authentication Events *279*
Table 10.5: User and User Group Events *279*
Table 10.6: Unit Events *279*
Table 10.7: Task Events *280*
Table 10.8: Unit Status Events *281*
Table 10.9: Access Control Events *281*
Table 10.10: Session Events *281*
Table 10.11: Top Navigation Bar Event Log Icons *283*
Table C.1: DSR Remote Operations Descriptions *303*
Table C.2: DSR Remote Operations Content Area Icons (Servers View) *304*
Table C.3: DSR Remote Operations Content Area Icons (Power View) *305*
Table D.1: VT Key and Keypad Numeric Codes *311*
Table D.2: VT100+ Function Key Support *312*
Table D.3: VT102 Receive Codes *312*
Table D.4: VT100 Special Keys and Control Keys *313*
Table D.5: VT100 ANSI Set and Reset Mode Cursor Keys *314*
Table D.6: VT100 PF1-PF4 Key Definitions *315*
Table D.7: VT100 ANSI Mode Control Sequences *315*

Table D.8: VT220 Encoding *319*
Table D.9: VT220 Decoding *320*
Table D.10: VT52 Encoding *322*
Table D.11: VT52 Decoding *322*
Table D.12: VT52 ANSI Mode Auxiliary Keypad Definitions *323*
Table D.13: VT320 Encoding *323*
Table D.14: VT320 Decoding *324*

CHAPTER 1

Product Overview

The DSView® 3.1.1 management software is a secure, web browser-based, centralized enterprise management solution that allows users to remotely access, manage, monitor and control target devices through Avocent managed appliances. A session may be launched to a target device with a single point of access.

Features and Benefits

Network rebooting and troubleshooting

The DSView management software uses industry standard IP connections so that you can easily troubleshoot a server, or even reboot it, from the Network Operations Center (NOC), from your desk or from any location in the world. With the DSView software, you can access all of your data center devices from a single screen - making complex network access and control remarkably easy.

Web-based access and control

The DSView management software provides secure “point-and-click” web browser-based access to control virtually any data center device using managed appliances from DSView software clients that may be located anywhere in the world.

The DSView software supports the following browsers:

- Microsoft® Internet Explorer version 6.0 SP1 and later
- Mozilla version 1.7.3 and later
- Firefox version 1.0 and later
- Netscape version 7.2 and later

It is recommended that the browser be kept up to date with the latest version.

A Video Viewer allows you to control the keyboard, monitor and mouse functions of individual target devices connected to a DS1800 digital switch or DSR® switch in real time. You may also use predefined global macros to perform actions within the Video Viewer window, or create new macros within the window for the device.

Devices connected to a CPS serial over IP network appliance or a CCM console management appliance may be accessed using the DSView Software Telnet Viewer. You may also use third party Telnet viewers.

Devices connected to a DSI5100 proxy appliance may be accessed using an IPMI Viewer window.

Secure authentication and communication

Secure Socket Layer (SSL) encryption may be used to encrypt data traveling within the DSView software system. Users may be authenticated using the DSView software server internal database, or using a Lightweight Directory Access Protocol (LDAP), Active Directory®, RADIUS (Remote Access Dial-In User Service), TACACS+ (Terminal Access Controller Access Control System) or Windows NT® domain external authentication server.

Creating and managing user permissions

The DSView management software provides centralized network access, control and security for managed appliances. A DSView software administrator may add, remove, delete and change settings for managed appliances and target devices, including assigning permissions and per-device contact information, which are stored on the DSView software server. A DSView software administrator may also assign unique permissions which allow individual users or a group of users access to units.

Proxy server access

The DSView management software also contains a proxy server feature that allows keyboard, video and switch (KVM) and serial sessions to be proxied through the DSView software server. When a session is initiated with a target device, the Video Viewer communicates using the Avocent Proxy Protocol (APP) and the DSView software server makes a direct connection to the appliance.

Virtual media

On certain DSR switch models, the DSRIQ-USB2 module and the virtual media feature allows the client workstation user to load files onto USB2-compatible target devices when the usual network resources are unavailable.

Mapping physical drives or image files on the client system as virtual drives on the target device can accommodate critical tasks required on the target device, such as operating system installation or recovery, BIOS updating and configuration backups.

System Components

The following components comprise a DSView software system.

DSView management software

The DSView management software resides on the DSView software server (host computer) and provides a web gateway and services for managing units (managed appliances and target devices) using a web browser. The gateway allows for IP-based video, serial management, Telnet Viewer, third party Telnet viewer or web browser sessions.

Users may connect to the DSView software server from DSView software clients and use the DSView Explorer window to communicate with the system.

DSView software server

The DSView software server contains the DSView management software that enables users to securely access, manage, monitor and control remote target devices through managed appliances. The DSView software server provides a centralized database repository for storing configuration and user, unit and system information. The software server also provides services for authentication, access control, logging events, monitoring and license management.

You may configure one or more spoke (backup) servers in addition to the hub server.

The hub server is responsible for maintaining the master copy of the database in a DSView software system. Only one server in a DSView software system may be configured as the hub server.

Spoke servers perform database replication with the hub server. The hub server acts as the coordinator for database replication between itself and all of the other spoke servers in a DSView software system. A hub server and a spoke server both offer the same DSView management software functionality to a user. The distinction of hub or spoke refers only to the database replication role that the server plays and not with the functionality that the server provides. Adding one or more spoke servers to a DSView software system provides redundancy and the ability to distribute DSView software functionality across multiple sites. For more information about replication, see *Replication* on page 77.

After the hub server and optional spoke server(s) are configured, you may create and configure the type of access levels for users within your network environment. You may also set up event logs to record full details of user access and other events.

DSView software client

A DSView software client is a computer with a web browser that may access the DSView management software installed on the DSView software server. A user may access and administer the DSView software server and units using the DSView software client.

Third party products

Third party products are not a part of the DSView software, but are supported for use with it.

External authentication servers - An external authentication server enables the DSView software server to broker authentication requests from users requesting access to the DSView software system.

SNMP managers - The SNMP (Simple Network Management Protocol) manager monitors the managed appliances and receives SNMP traps from the DSView software on the server. An example of an SNMP manager is the HP OpenView product.

Third party Telnet viewers - A third party Telnet viewer may be used for serial sessions instead of the DSView software Telnet Viewer.

Supported Units

A managed appliance may provide KVM, serial over IP or IPMI connectivity to target devices. The DSView management software supports the following managed appliances.

CPS and CCM appliances

The CPS and CCM appliances allow users to access serially attached devices over a standard TCP/IP connection using a Telnet Viewer or a third party Telnet viewer. The DSView software supports:

- CPS810 and 1610 serial over IP network appliances
- CCM850, 1650 and 4850 console management appliances

DSView software clients communicate with target device serial ports using a Telnet connection between the client and the appliance. The appliance converts the Telnet data to a serial stream, which is then sent to the target device.

For management functions, the DSView software client uses HTTPS (Hypertext Transfer Protocol with SSL encryption) to send a request to the DSView software server, which then sends a command to the managed appliance. The appliance then performs the requested management function.

CPS and CCM appliances also support SPC target devices.

DS1800 digital switches and DSR switches

The DS1800 digital switch and DSR switches are managed appliances that allow KVM signals to be transmitted over a standard TCP/IP network connection. Some DSR switches may alternately be connected using a modem, which provides benefits for branch offices such as low cost and dial-up performance.

The DSView software supports DS1800 digital switches and the following DSR switch models:

800, 1010, 1020*, 1021*, 1022*, 1024*, 1030, 1031, 1161, 2010, 2020*, 2030*, 2035*, 2161, 4010, 4020*, 4030*, 4160, 8020*, 8030*, 8035*

* These models contain a modem port for use with the DSR Remote Operations Software. See *DSR Remote Operations Software* on page 301 for more information.

A target device is first attached to DSRIQ module, which is then attached to a DSR switch. A DSRIQ module converts KVM signals to Application Data Protocol (ADP) packets that are sent between the DSRIQ and the managed appliance.

DSView software clients communicate with target devices ports using a Video Viewer connection between the client and the managed appliance. The managed appliance converts packets received from the Video Viewer into packets that are sent and may be read by a DSRIQ module. The DSRIQ module then converts the data to KVM signals that are sent to target devices.

For management functions, the DSView software client uses HTTPS to send a request to the DSView software server, which sends a command to the managed appliance. The managed appliance then performs the requested management function.

These managed appliances also support SPC devices.

The DS1800 digital switches and DSR switches allow the cascading of legacy analog KVM switches from DS1800 digital switch or DSR switch ports, which may be managed in a DSView software system.

The following legacy KVM switches are supported:

- AutoView 200-4, 200-8, 400-4, 400-8, 416, 424 and 2000-AM switches (these switches must be Flash upgraded to be added to a DSView software system)
- OutLook 140ES, 180ES, 280ES, 1160ES, 2160ES and 4160ES switches

PEM cascade devices are not supported.

DSI5100 proxy appliances

The DSI5100 appliance is an IPMI proxy network product that securely interfaces with IPMI-capable target devices to access, aggregate and report IPMI information in the DSView software. DSView software clients interface with IPMI 1.5 target devices connected to the DSView software system.

The DSI5100 appliance collects baseboard management controller (BMC) data from internal IPMI 1.5 target device sensors and allows you to display a variety of IPMI information.

A DSI5100 appliance may be attached to only one DSView software system at a time.

EVR1500 environmental monitors

The EVR1500 environmental monitor is a managed appliance that uses standard web browser communication between DSView software clients and a DS1800 digital switch or DSR switch.

Generic appliances

Generic appliances manage data center devices such as routers. These devices may be managed within a DSView software system by launching a standard web browser to the device URL or by opening a Telnet session.

Embedded units

Using the DSView software, you may add/delete, configure/display properties, and launch video sessions to the following versions of third party embedded units:

- IBM® ASM (Advanced System Management) RSA II (Remote Supervisor Adapter II) - Version 5, Build GRE132AUS
- DRAC 4 (Dell™ Remote Access Controller) - Version 1.0, Build 06.14
- Compaq iLO (Integrated Lights-Out) - Version 1.20
- NEC IPF (Itanium Processor Family) - Version 0.5.1.20

For management functions (other than launching video sessions) that are not performed by the DSView software, see the documentation for the unit.

Target devices

Target devices encompass a wide range of data center components such as servers and routers that a DSView software administrator may manage virtually through the DSView software system. A target device is added automatically to your DSView software system when the supported managed appliance is added. A target device may also be added individually when not attached to a supported managed appliance.

SPC devices

An SPC device is a type of target device that may be cascaded from a CPS or CCM appliance serial port or connected to an SPC port of a DS1800 digital switch or DSR switch. One or more CPS or CCM appliance serial ports may be attached to the SPC power control device. When a DSView software client sends a power control request to a target device, an HTTPS request is sent to the DSView software server, which then sends a command to the appliance. The command is converted and serially sent to the SPC device. The SPC device then turns the appropriate power outlet on or off.

Figure 1.1 illustrates an example system configuration using the DSView management software. For information about the TCP ports that the DSView software uses, see *TCP and UDP Ports* on page 292.

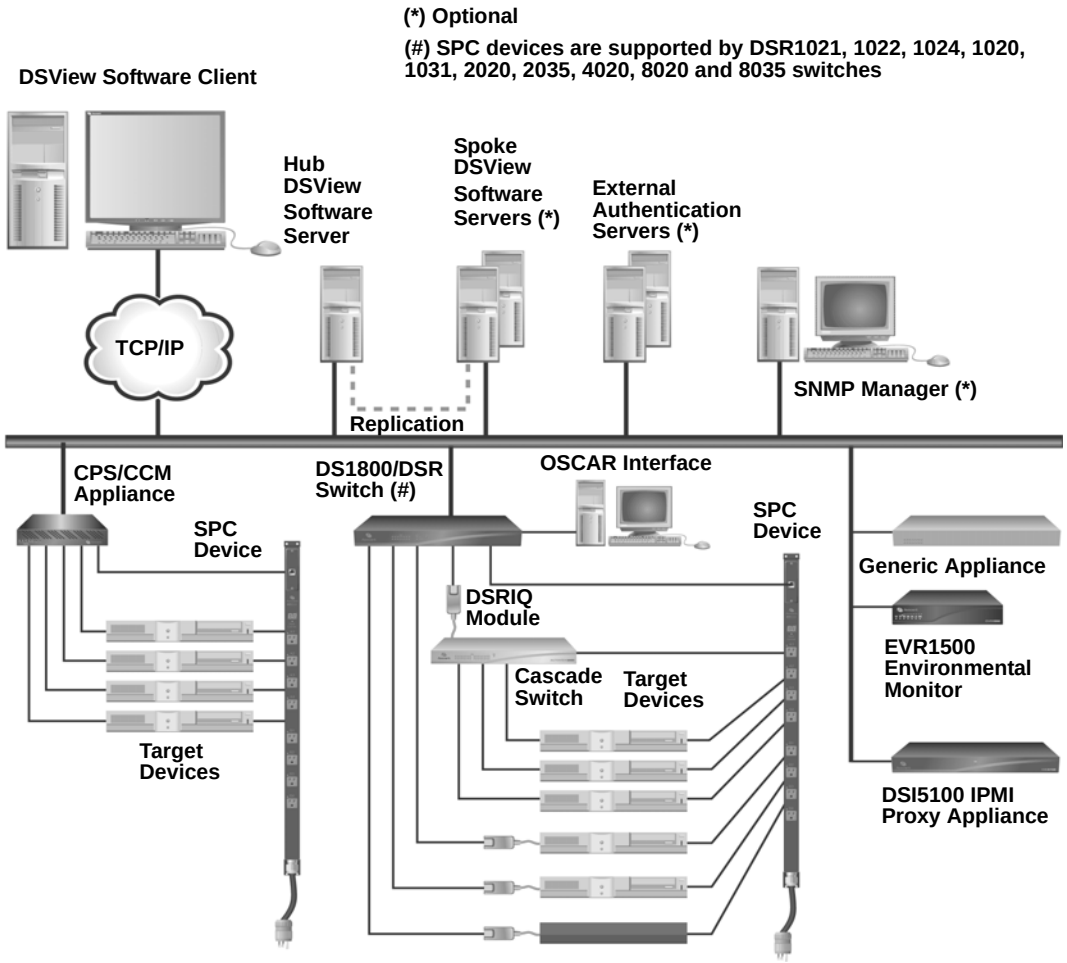


Figure 1.1: Example System Configuration Using the DSView Management Software

About the DSView Explorer Windows

When a user has been logged in and authenticated, the Avocent DSView Explorer window appears. From the DSView Explorer window, users may view, access and manage units. Custom groupings may be created for managed appliances. The window may also be used to specify system settings, display report information and change profile settings.

Figure 1.2 shows the DSView Explorer window areas.

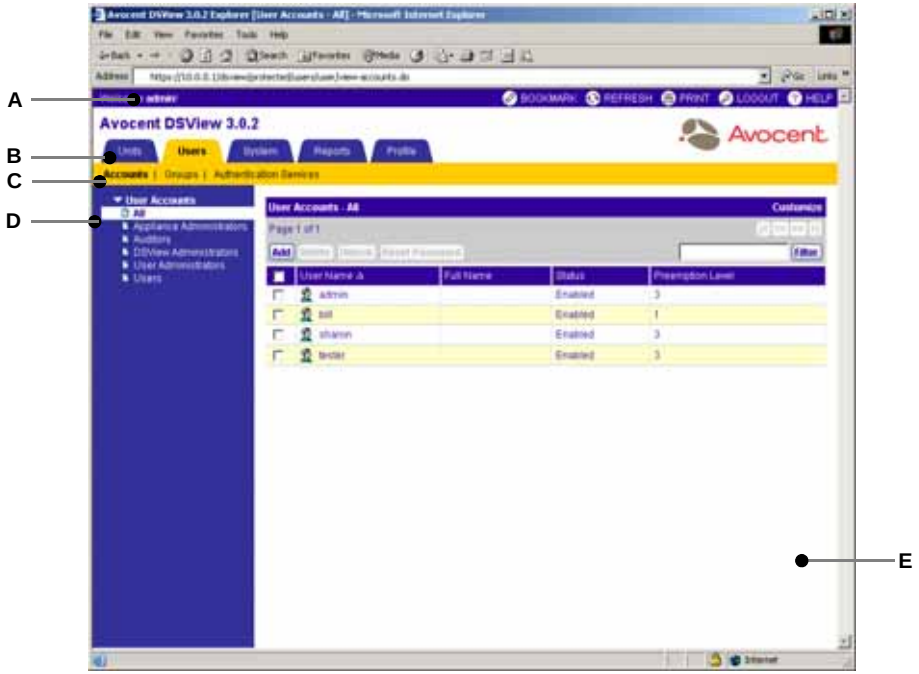


Figure 1.2: Avocent DSView Explorer Window

Table 1.1 describes some of the DSView Explorer window areas.

Table 1.1: DSView Explorer Window Area Descriptions

Letter	Description
A	Top option bar - Use the top option bar to bookmark a DSView management software window, refresh the display of a DSView management software window, print a web page, log out of a software session or access online help. The name of the logged in user appears on the left side of the top option bar.
B	Tab bar - Use the tab bar to display and manage units, user accounts, reports, system settings and user profiles.

Table 1.1: DSView Explorer Window Area Descriptions (Continued)

Letter	Description
C	Top navigation bar - The selections in the top navigation bar vary, depending on the active tab in the tab bar. These options display in the side navigation bar
D	Side navigation bar - Use the side navigation bar to display the system information you wish to display or edit, which displays in the content area. The side navigation bar also contains icons in the top left corner which, when clicked, expand or collapse all nodes.
E	Content area - Use the content area to display or make changes to the DSView software system.

When a Units View is displayed, the unit entries often contain icons.

- Target device icons may be changed. See *Changing Unit Overview Information* on page 95 for more information.
- Managed appliance icons, which are listed in Figure 1.2, may not be changed.

Table 1.2: Managed Appliance Icons

Icon	Description
	CPS or CCM appliance
	DS1800 digital switch, DSI5100 appliance, DSR switch or embedded unit
	EVR1500 environmental monitor
	Generic appliance

Accessing target devices

Target devices (TDs) that may be accessed system-wide are displayed in a Unit Views window. Table 1.3 lists the Action links (connection methods) that may be be used to initiate sessions with a target device connected to a managed appliance, launch a session to an embedded unit or to display a generic appliance or EVR1500 environmental monitor.

Table 1.3: DSView Explorer Window Links

Clicking this link	Displays	Associated with
Browser session	Web browser	EVR1500 environmental monitors, generic appliances, standalone TDs and TDs attached to DS1800 digital switch, CPS appliance, CCM appliance, Compaq iLO embedded unit or DSR switch channels or ports

Table 1.3: DSView Explorer Window Links (Continued)

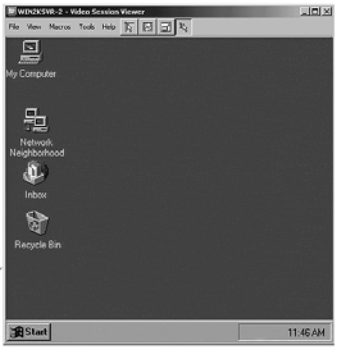
Clicking this link	Displays	Associated with
IPMI Session	IPMI Viewer window	IPMI 1.5 TDs
Telnet Session	Telnet Viewer window or third party Telnet viewer window	EVR1500 environmental monitors, generic appliances, TDs and TDs attached to DS1800 digital switch, CPS appliance, CCM appliance or DSR switch channels or ports
Serial Session	Telnet Viewer window	TDs attached to CPS or CCM appliance serial port
KVM Session	Video Viewer window	TDs attached to DS1800 digital switch or DSR switch channels or ports
Virtual Media Session	Video Viewer window	DSR1030, 1031, 2030, 2035, 4030, 8030 and 8035 switches
Reserved Virtual Media Session	Video Viewer window	DSR1030, 1031, 2030, 2035, 4030, 8030 and 8035 switches
Exclusive KVM Session *	Video Viewer window	TDs attached to a DS1800 digital switch or DSR switch channels or ports
<name> Embedded Session	Viewer window	Supported versions of IBM ASM RSA II, DRAC 4 and NEC IPF embedded units.

* An Exclusive KVM Session link appears only when the alternate actions arrow is selected in the Action column.

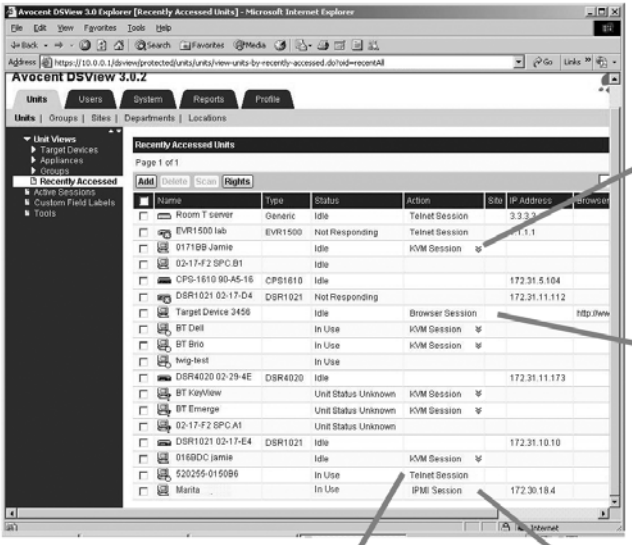
If multiple connection methods are available, an alternate actions arrow will appear to the right of the action. Clicking the alternate action arrow will display a list of other actions, in descending order of priority. These alternate actions may then be selected to launch the corresponding connection type.

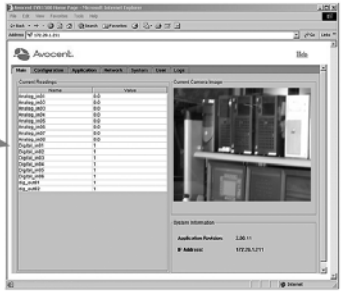
Figure 1.3 illustrates using some of the Action links.

Access the Video Viewer window by clicking *KVM Session* in a Unit Views window.

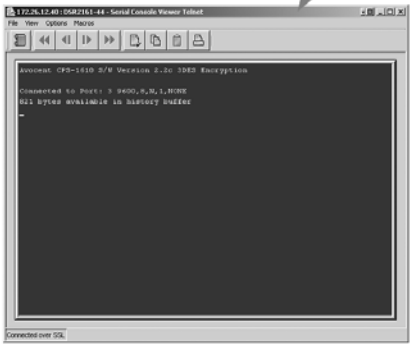


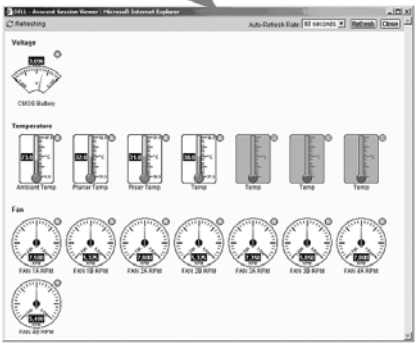
DSView Explorer Window





Access a web browser by clicking *Browser Session* in a Unit Views window.





Access a Telnet Viewer window by clicking *Telnet Session* or *Serial Session* in a Unit Views window.

Access an IPMI Viewer window by clicking *IPMI Session* in a Unit Views window.

Figure 1.3: Launching DSView Management Software Sessions

You may also connect to a target device attached to a DS1800 digital switch or DSR switch with a KVM session from the Unit Overviews window. See *Changing Unit Overview Information* on page 95 for more information.

Using the side navigation bar

The side navigation bar may be used to display windows to specify settings or perform operations. The contents of the side navigation bar may vary, depending on the tab bar selection, top navigation bar selection and the window that is displayed. Figure 1.4 illustrates some of the side navigation bar features.

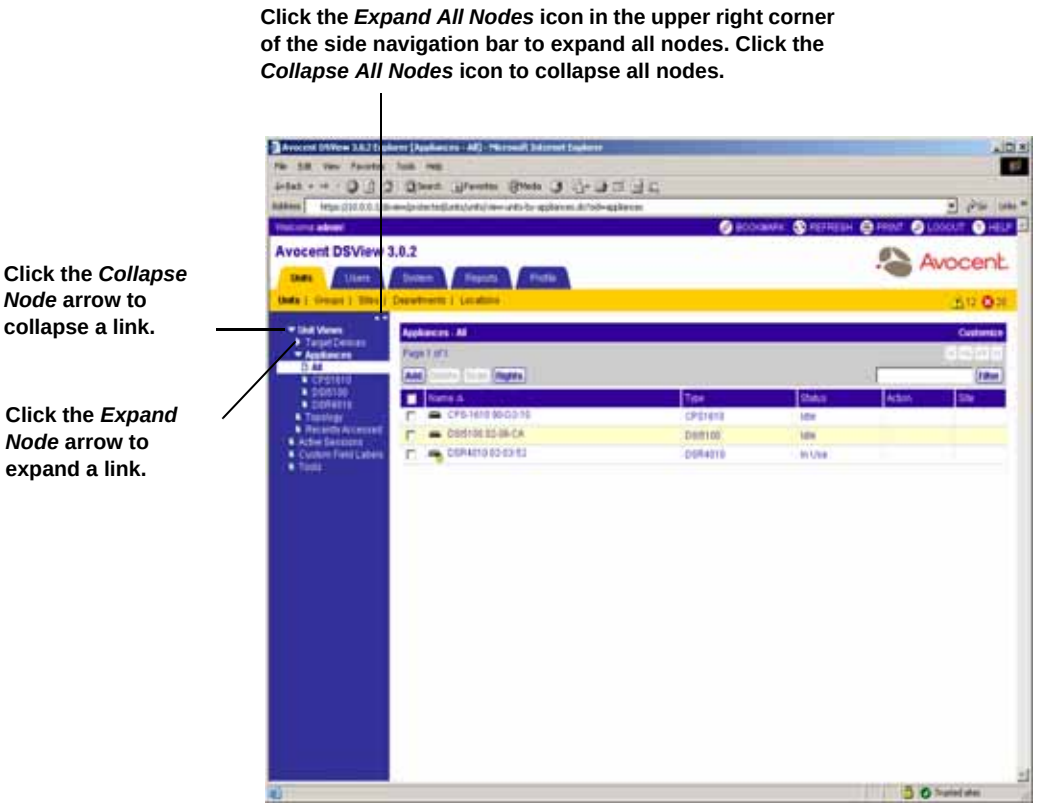

Click the *Expand All Nodes* icon in the upper right corner of the side navigation bar to expand all nodes. Click the *Collapse All Nodes* icon to collapse all nodes.
Click the *Collapse Node* arrow to collapse a link.
Click the *Expand Node* arrow to expand a link.
Avocent DSView 3.0.2
Avocent

Figure 1.4: Side Navigation Bar

Table 1.4 describes the icons that may appear in the side navigation bar.

Table 1.4: Side Navigation Bar Icons

Icon	Description
	Expand All Nodes - Click this button in the upper right corner of the side navigation bar to expand all nodes and display additional links.
	Collapse All Nodes - Click this button in the upper right corner of the side navigation bar to collapse all nodes and their links.
	Collapse Node - Click this button to collapse an opened tree branch in the side navigation bar and its links.
	Expand Node - Click this button to expand a closed tree branch in the side navigation bar and display its links.

You may choose whether an expanded node will collapse when another *Expand Node* arrow is selected. See *Changing user options* on page 19 for more information.

Clicking on a link that does not contain an arrow will display its corresponding window. Some windows contain additional links, which may display another window and a different side navigation bar.

Sorting information in a window

The order of rows in a list displayed in a DSView Explorer window may be changed by clicking the heading of one of the displayed columns. When you click a column heading, the order of the list rows will change to alphabetically ascending, based on that column. If you click the column heading a second time, the order will change to an alphabetically descending order. An up arrow indicates ascending order and a down arrow indicates descending order.

If you are using the Topology view, sorting is first performed on parents (managed appliances) and then on the children (target devices) beneath the managed appliances.

Filtering information in a window

Some DSView software windows allow you to filter list information by providing a text string that will be used to retrieve matching items. Filtering is useful if you have many target devices or other items that extend over many pages. Windows that allow filtering contain a text field and Filter button in the upper right portion of the window, as shown in Figure 1.2.

Filtering is performed over the entire list of items, not just those displayed in the current window, and can provide a shorter, more exact list of items. When filtering is performed, the text in every row and column in the window is searched for the specified text string. For example, you may wish to perform filtering to list only DSR1021 switches in the Name column, target devices with KVM connections in the Action column, CPS appliances that are idle in the Status column and so on.

If the Topology window is filtered, both parent and child units will display in the filtered view. For example, if you filter for a child named target device 1 that is attached to a DSR1021 switch, target device 1 will appear below the DSR1021 switch in the filtered view.

When filtering, you may use an asterisk (*) before and/or after text strings as a wildcard. For example, typing **emailserver*** and clicking *Filter* will display items with emailserver at the beginning (such as emailserver, emailserverbackup). Typing ***emailserver*** and clicking *Filter* will display items containing emailserver in any part of the name (such as emailserver, emailserverstore, tdemailserver, tdemailserver1).

Table 1.5 lists the ways you may specify text strings for filtering.

NOTE: Searches are not case sensitive.

Table 1.5: Filter Field Text Strings

Typed in the Filter Field	Results
<String>	Entering a string displays a filtered list of items that contain the 'word' (that is, it will find matching strings that are followed by anything other than a letter or number). For example, typing **email** will list any items that contain the string email, followed by a space or punctuation mark. If you enter multiple words separated by spaces but without logical operators, OR is assumed, and each word is treated separately. For example, typing **email server** will display items containing email or server.
"<String>"	Surrounding the string with quotation marks displays a filtered list of items containing the exact string, including spacing and punctuation. For example, typing **"email server"** will display items that contain email server. The DSView software will provide a closing quotation mark if it is omitted.
<String1> AND <String2>	Using the AND logical operator displays the items that contain both strings. For example, typing **email and server** will display items named email-server-3, email-server-2, server email and so on.
<String1> OR <String2>	Using the OR logical operator displays the items that contain at least one of the strings. For example, typing **email or server** will find any items that contain the string email or the string server.
(<String>)	Parentheses may be used to override the default (left to right) order of precedence during evaluation of a filter string. For example, searching for **email and server or service** would be the equivalent of ((email and server) or service), which may not be the intended search. The user may choose instead to change the order of precedence by grouping the search terms with parentheses, such as **(email) and (server or service).**
NOT <String>	Preceding the string with NOT displays all items that do not contain the string. For example, typing **not email** will display all items except those containing email (email, email server, email-server-1 and so on will not display).

To filter the list in the current window:

1. From a window containing a Filter field, type a text string in the field. Searches are not case sensitive.
2. Click *Filter*. A filtered list of the information in the window will be displayed.
3. Click *Clear* to return to a non-filtered list.

Saving information in a window

When you change information in a DSView Explorer window, you must click *Save* in order to apply the changes. By default, a message box will appear if you click *Close* or try to exit the window by clicking a link in the top bar, top navigation bar or side navigation bar without first clicking *Save*.

Clicking *OK* in the message box will exit the current window without saving the changes. If you wish to save the changes you have made, click *Cancel* in the message box and then click *Save* in the window.

You may choose whether or not to be reminded to save changes made to windows before exiting them. See *Changing user options* on page 19 for more information.

Using the Customize link in windows

DSView Explorer windows that contain a Customize link allow you to change the following information:

- Which columns of information are displayed
- The number of items displayed per page in the window
- Showing units that have been hidden (Unit Views windows)

The items available for customizing and methods for changing them will vary, depending on the window you choose to customize. Although the items that appear in windows may vary (depending on the window you customize), the items that do appear are modified identically regardless of the window from which you clicked the *Customize* link.

To customize a window using the Customize link:

1. In a window containing a Customize link in the upper right corner, click the link. A View Customization window will open.
2. Customize the window.

   To add a field to the window display:

   a. Select the field in the Available Fields list. Multiple fields may be selected by pressing **Ctrl** or **Shift** while clicking on the field names.

   b. Click *Add*. The field(s) will be moved to the Fields to Show list.

   To change the order that fields display from left to right in the window:

   a. Select a field in the Fields to Show list.

b. Use the up or down arrow to change its order in the list. Multiple fields may be selected by pressing **Ctrl** or **Shift** while clicking on the field names.

To remove a field from displaying in the window:

a. Select the field from the Fields to Show list. Multiple fields may be selected by pressing **Ctrl** or **Shift** while clicking on the field names.

b. Click *Remove*. The field(s) will be moved to the Available Fields list.

To specify the number of items that appear in a window, use the arrow keys to specify a number or type a number in the Items per Page field.

To show hidden items in a window:

a. Click *Show hidden items*.

b. Select the *Visibility* column from the Available Fields list and click *Add* to move Visibility to the Fields to Show list.

3. Click *Save* when you are finished.
4. Click *Finish*. The window being customized will open with the modifications.

Displaying pages

Multiple page DSView Explorer windows contain navigation buttons which may be used to quickly move among pages. Table 1.6 describes the page navigation buttons.

Table 1.6: DSView Explorer Page Navigation Buttons

Button	Description
	First Page - Navigates to the beginning of a list displayed in a window.
	Previous Page - Navigates to the previous page of a list displayed in a window.
	Next Page - Navigates to the next page of a list displayed in a window.
	Last Page - Navigates to the end of a list displayed in a window.

The number of items that display in a window page is specified by using the *Customize* link. The current page and total number of pages appear in the top left corner of the window.

The navigation buttons are enabled only if there are enough pages available to make them necessary.

Bookmarking a window

Many DSView Explorer windows contain a bookmark icon and text in the top option bar. Bookmarking a window will add a link to the window in the Favorites drop-down menu. You may select the link at any time to quickly access the bookmarked window.

If you bookmark a window and information related to the window changes, this new information will appear in the window when you next display the bookmarked window. For example, if you bookmark the Recently Accessed window and then access other units, the bookmarked window will contain these other units the next time you display the bookmarked page.

If you click *BOOKMARK* or the bookmark icon after the DSView software server session has timed out, the User Login window will open and you must log in again. After you log in, you will be redirected to the bookmarked page.

To bookmark a window:

1. In the top option bar, click *BOOKMARK* or the bookmark icon. The Add Favorite dialog box will appear.
2. If you wish, type a name for the window. You may also click the *Create in* button to create or specify a folder in which to place the window.
3. Click *OK* to close the Add Favorite dialog box.

Printing a window

All DSView management software windows contain a print icon and text in the top option bar.

To print a DSView software window:

1. In the top option bar, click *PRINT* or the print icon. The Print dialog box will appear.
2. Specify the options you wish to use for printing the DSView management software window.
3. Click *Print* to print the DSView management software window and close the Print dialog box.

Refreshing a window

A DSView Explorer window may be refreshed at any time by clicking *REFRESH* or the refresh icon in the top option bar.

By default, status information automatically refreshes every 30 seconds. The automatic refresh interval may be changed or disabled. See *Changing user options* on page 19 for more information.

Using keyboard commands

In addition to using your mouse, certain keyboard commands may be used to select and change items in DSView Explorer windows.

Table 1.7 lists general keyboard commands that may be used in DSView Explorer windows.

Table 1.7: General Keyboard Commands

Key	Description
Tab	Transfers focus to the next control in the window, including the calendar
Shift-Tab	Transfers focus to the previous HTML control

Table 1.8 lists the keyboard commands that may be used in DSView Explorer windows when a calendar is enabled and has focus.

Table 1.8: Calendar Keyboard Commands

Key	Description
Enter or Space	Displays or closes the calendar.
Esc	Closes the calendar.
Page Up	Decrements the month by one month and selects the first day of the month.
Page Down	Increases the month by one month and selects the first day of the month.
Right Arrow	Increments the day by one day. If the last day of the month is selected and the **Right Arrow** key is pressed, the month is incremented to the next month.
Left Arrow	Decrements the day by one day. If the first day of the month is selected and the **Left Arrow** key is pressed, the month is decremented to the previous month.
Up Arrow	Decrements the weekday by one week. If the first weekday type of the month is selected and the **Up Arrow** key is pressed, the month is decremented to the previous month.
Down Arrow	Increments the weekday by one week. If the last weekday type of the month is selected and the **Down Arrow** key is pressed, the month is incremented to the next month.

Table 1.9 lists the keyboard commands that may be used in DSView Explorer windows when a spinner is enabled and has focus.

Table 1.9: Spinner Keyboard Commands

Key	Description
Up Arrow	Increments the spinner number by one
Down Arrow	Decrements the spinner number by one

Profiles

Profile information contains features and tasks that may affect actions when using the DSView Explorer. These include:

- User options
- Color scheme
- Changing a password
- Enabling/disabling use of a third party Telnet application
- Specifying a user certificate
- Specifying a user SSH key

Changing user options

User options enable/disable features or affect actions when using the DSView Explorer.

To change user options:

1. Click the *Profile* tab. Preferences will automatically be selected in the top navigation bar. Options will automatically be selected in the side navigation bar and the Options window will open.
2. Select *Automatically collapse navigation tree nodes* for the currently-expanded tree node in the side navigation bar to be collapsed when another tree node is selected.

   -or-

   Uncheck *Automatically collapse navigation tree nodes* for any expanded tree nodes in the side navigation to remain expanded. (This is the default value.)
3. Select *Skip prompt when leaving pages with unsaved changes*, if you do not want a message box to appear reminding you to save modified information when you leave a window.

   -or-

   Uncheck *Skip prompt when leaving pages with unsaved changes* if you wish for a message box to appear reminding you to save modified information when you leave a window.
4. Select a refresh rate. By default, windows automatically refresh every 30 seconds. You may specify another rate from five seconds to five minutes. If you select *Never*, windows will only be refreshed when you click the *REFRESH* icon or text in the top option bar.
5. Select *Skip Welcome Pages in Wizards* to disable the welcome page of all wizards.

   -or-

   Uncheck *Skip Welcome Pages in Wizards* to enable the welcome page in all wizards.
6. Click *Save*.

Changing the color scheme

When the color scheme is changed, it is changed only for the logged in user. Each user may specify their own color scheme.

To change the color scheme of the DSView Explorer:

1. Click the *Profile* tab.
2. Click *Preferences* in the top navigation bar.
3. Click *Color Scheme* in the side navigation bar. The Color Scheme window will open.
4. Click a color scheme to use.
5. Click *Save*. The color scheme will be applied to the DSView Explorer window.

Changing your password

Users may change their passwords only if the Administrator has set appropriate permissions See *Adding User Accounts* on page 153 for more information.

By default, passwords must contain at least three characters and will never expire. A DSView software administrator may specify a different minimum character length and an expiration date. See *Managing Authentication Services* on page 58 for more information.

To change your password:

1. Click the *Profile* tab.
2. Click *Preferences* in the top navigation bar.
3. Click *Change Password* in the side navigation bar. The Change Password window will open.
4. Type your current password.
5. Type and confirm the new password.
6. Click *Save*.

Enabling/disabling use of a third party Telnet application

You may choose to use a third party Telnet application instead of the DSView software Telnet Viewer for serial sessions. Once you configure a third party application in a profile, that application will be used whenever a serial session is launched.

You may also return to using the DSView software Telnet Viewer by disabling use of the third party Telnet application.

To enable use of a third party Telnet application:

1. Click the *Profile* tab. Preferences will automatically be selected in the top navigation bar.
2. Click *Applications* in the side navigation bar.
3. Check the *Enable 3rd Party Application* checkbox.
4. Enter the path and executable name of the application (maximum 256 characters) in the Serial Application field.
5. Specify any of the following parameters (up to 128 characters) in the Command Line Arguments field. When the serial session is launched, the actual values will be substituted.

   %ADDRESS% - The IP address will be substituted.

%PORT% - The port number will be substituted.

%TNAME% - The target name of the unit will be substituted.

6. If the third party application does not automatically launch a command window, enable the *Launch in Command Window* checkbox.
7. Click *Save*.

To disable use of a third party Telnet application:

1. Click the *Profile* tab. Preferences will automatically be selected in the top navigation bar.
2. Click *Applications* in the side navigation bar.
3. Uncheck the *Enable 3rd Party Application* checkbox.
4. Click *Save*.

The DSView Telnet Viewer will now be used when a serial session is launched.

Specifying a user certificate

NOTE: This property may only be modified for users using internal authentication. See *Managing Authentication Services* on page 58 for more information.

A user may specify a certificate, if the administrator has allowed it.

As an alternative to this method, the administrator may specify the certificate in the user account properties. See *Changing certificates associated with users* on page 156 for more information.

To enable user settable certificates:

NOTE: Only Administrators may access this procedure.

1. Click the *System* tab.
2. Click *User Credential Properties* in the side navigation bar.
3. Enable the *Allow user to set own certificate* checkbox.
4. Click *Save*.

To specify a user certificate:

NOTE: A user may access this procedure only if an Administrator has previously enabled it.

1. Click the *Profile* tab. Preferences will automatically be selected in the top navigation bar.
2. Click *Credentials* in the side navigation bar, then click *Certificate*.
3. Type the path and name of the certificate.

   -or-

   Use the *Browse* button and select a certificate using the Choose File dialog box.
4. Click *Save*. An updated Certificate window will open.

Specifying an SSH key

A user may specify an SSH key, if the administrator has allowed it.

As an alternative to this method, the administrator may specify the SSH key in the user account properties. See *Specifying a user SSH key* on page 157 for more information.

To enable user settable SSH keys:

NOTE: Only Administrators may access this procedure.

1. Click the *System* tab.
2. Click *User Credential Properties* in the side navigation bar.
3. Enable the *Allow user to set own SSH key* checkbox.
4. Click *Save*.

To specify an SSH key:

NOTE: A user may access this procedure only if an Administrator has previously enabled it.

1. Click the *Profile* tab. Preferences will automatically be selected in the top navigation bar.
2. Click *Credentials* in the side navigation bar, then select *SSH Key.*
3. Type the 1-256 character name of the file containing the public SSH key that was generated by a third party key generator.

   -or-

   Use the *Browse* button and select a certificate using the Choose File dialog box.
4. Click *Save*. An updated SSH Key window will open. The SSH key file will be uploaded to the DSView software server for use in authenticating the user.

Built-in User Groups

The user group to which a user belongs determines the actions the user may perform during a DSView management software session. A user may be assigned to any of the following five built-in user groups when they are added to the DSView management software system:

- DSView software administrators
- Appliance administrators
- Auditors
- User administrators
- Users

Table 1.10 lists the operations that may or may not be performed by users that are members of a build-in user group.

Table 1.10: Built-in User Groups and Allowed Operations

Operations	Built-in User Groups				
	S/W Admin.	User Admin.	Appl. Admin.	Auditors	Users
Configure DSView software system-level settings	Yes	No	No	No	No
Backup and restore the DSView software database	Yes	No	No	No	No
Register the DSView software spoke server	Yes	No	No	No	No
Define, display and change user account custom field labels	Yes	Yes	No	No	No
View, add, change and delete external authentication servers	Yes	Yes	No	No	No
Configure event log retention time	Yes	No	No	Yes	No
Configure events that are logged to the event log	Yes	No	No	Yes	No
View and delete events in an event log	Yes	No	No	Yes	No
Access events from the top navigation bar	Yes	No	No	Yes	No
View, add, change, import and delete DSView software	Yes	Yes	No	No	No
View user account custom field labels and properties	Yes	Yes	No	No	No
View, add, change and delete user-defined user groups	Yes	Yes	No	No	No
Reset account passwords	Yes	Yes	No	No	No
Configure the preemption level for an added user group	Yes	Yes	No	No	No

Table 1.10: Built-in User Groups and Allowed Operations (Continued)

Operations	Built-in User Groups				
	S/W Admin.	User Admin.	Appl. Admin.	Auditors	Users
Change the preemption level for users and user groups	Yes	Yes	No	No	No
View and select external authentication server names	Yes	Yes	No	No	No
View, add, change and delete unit entries	Yes	No	Yes	No	No
View, add, change and delete unit groups	Yes	Yes	Yes	No	No
Configure unit access control settings	Yes	Yes	No	No	No
Add, change and delete sites, departments and locations	Yes	No	Yes	No	No
View and select user account names and user group names	Yes	Yes	No	No	No
Change your own password	Yes	Yes	Yes	Yes	Yes
View managed appliances that have one or more access rights including status or appliance status	Yes	Yes	Yes	No	Yes

Users may also be added to user-defined user groups; see *Managing User Groups* on page 163.

Preemption Levels

The preemption level of users determines whether they may interrupt or disconnect another user's serial or video (KVM) session with a target device. This also applies to virtual media sessions, which are initiated from the Video Viewer.

DSView software administrators and user administrators may specify the preemption level for user accounts or user-defined user groups when an account or group is created. The preemption level may be changed later. See *Changing the preemption level for a user* on page 159 or *Displaying and changing user group properties* on page 166 for more information.

By default, the preemption level used by the DSView management software (the effective user preemption level) is the highest level of all of the user groups to which the user belongs. Preemption levels range from 1-4, with 4 being the highest level. For example, a user or a user

group with a preemption level of 4 may preempt other level 4 users or user groups, as well as those with a level 1, 2 or 3 setting.

Table 1.11: User and User Group Preemption Levels

Preemption Level	Description
4	The default preemption level for a new local user of a DS1800 digital switch, CPS appliance, CCM appliance or DSR switch.
3	The default preemption level for the DSView software administrator and appliance administrator user groups by the DSView management software.
2	The default preemption level for the user administrator user group.
1	The default preemption level for the users and auditors groups.

The preemption levels may be used in the following ways:

- User preemption level - This is the preemption level assigned to a user by a DSView software administrator or user administrator. If this value is larger than the highest preemption level of the user group to which the user belongs, the value will be used as the effective user preemption level.
- Group preemption level - This is the preemption level assigned to user groups to which the user belongs. If the user is assigned to multiple user groups with different preemption levels, this will be the preemption level of the user group with the highest level. For example, if a user belongs to the administrators (level 3) and auditors (level 1) user groups, this value will be defined as 3. If this value is larger than the highest preemption level of the user, the value will be used as the effective user preemption level.
- Effective user preemption level - This is the largest value between the user and group preemption level, and is the actual preemption level that will be recognized by the DSView software when the user attempts to preempt another user's session. For example, if user belongs to the auditors group (level 1) but is assigned a user preemption level of 4, the user will have an effective user preemption level of 4. Although a member of the auditors group, this user would also be able to preempt the session of a user belonging to the administrators or appliance administrators user groups.

An administrator or user administrator may also specify an OSCAR graphical user interface preemption level that is applied to users accessing target devices through the OSCAR interface. See *Managing and changing port settings* on page 111 for more information.

Other Features and Considerations

This section includes information that is useful when using the DSView software with:

- Internet Explorer
- Certificates

- Integrated Windows Authentication®
- A firewall
- A Virtual Private Network (VPN)
- A Network Address Translation (NAT) device

Configuring Internet Explorer

When the Internet Explorer web browser is used, specific settings are required to enable the DSView software to operate correctly.

- SSL (Secure Sockets Layer) certificates - Used for secure authentication between the DSView software client and DSView software hub server.
- ActiveX controls - Used to display Telnet application, serial and KVM sessions.
- Security Zones - Used to control the actions that may be performed within Internet Explorer. For example, the operation of JavaScript, which is used by the DSView software, is dependent on security zone settings.
- Advanced Internet options - Used for miscellaneous settings that enhance the use of the DSView software.

Correcting certificate security alerts

The DSView management software uses SSL to securely communicate between the DSView software hub server and DSView software clients. SSL provides secure authentication using certificates, which is data that identifies the PC with which communication will occur. A certificate is typically verified by another certificate from a trusted certificate authority. See *Using certificates* on page 31 for more information.

When the DSView management software is initially installed, it generates a self-signed certificate for use with DSView software clients. An administrator may replace the generated certificate with a certificate signed by a trusted third party. If the generated certificate is not replaced, the web browser will prompt a user whether to trust the generated certificate when a DSView software client session is started.

Three tests are performed on a certificate each time a DSView software client connects to the DSView software hub server:

- Does the client web browser trust the certificate issuer?
- Has the certificate expired?
- Does the name on the DSView software server certificate match the name the DSView software client used to access the DSView software server?

A Security Alert dialog box will appear if the answer to any of the three questions is No. To prevent the Security Alert message box from appearing when you connect to a the DSView software hub server, all three questions must be answered Yes.

To correct certificate security alerts for client and hub server connections:

1. From the DSView software client server, connect to the DSView software hub server using Internet Explorer. The Security Alert dialog box will appear.
2. In the Security Alert dialog box, click *View Certificate*. The Certificate dialog box will appear.

   If you click *No*, a connection will not be made with the DSView software hub server and the DSView software User Login window will open. If you click *Yes*, a connection will be made with the DSView software hub server and the DSView software Login Screen will appear, but the Security Alert dialog box will continue to appear each time you connect to the hub server.
3. Click *Install Certificate* to install a new certificate. See the Internet Explorer documentation for more information.
4. Once the certificate is installed, ensure that the time setting on the DSView software client PC is within the Valid from...to... dates and that the Issued to and Issued by fields exactly match.

   Invalid to...from dates typically occur when the DSView software is installed on a server that is set to an invalid time. When a DSView software client that is set to a valid time connects to the DSView software server that is set to an invalid time, a “The security certificate date is invalid” warning will appear in the Security Alert dialog box.

Serial session security alerts

The Serial Session Viewer, which is used during a serial session, is a Java-based applet. Three certificate tests are performed by Java when the DSView management software connects to a serial device:

- Does the serial device trust the certificate issuer?
- Has the certificate expired?
- Does the name on the serial device certificate match the name of the DSView software hub server certificate?

A Warning - Security dialog box will appear if the answer to all three questions is No. If the answers to the first two questions are Yes and the last question is No, a Warning - HTTPS dialog box will appear. To prevent either of these warning dialog boxes from appearing when you connect to a serial device, all three questions must be answered Yes.

To correct certificate security alerts when connecting to a serial session:

1. From a Unit Views window Action column for a CPS or CCM appliance, click *Serial Session*.

   -or-

   From a Unit Views window, click on the name of a CPS or CCM appliance. *Overview* will automatically be selected, the name of the appliance will appear at the top of the side navigation bar and the Overview window will open. Click the *Serial Session* icon or text.
2. If a Warning - Security dialog box appears, continue to step 3.

If the certificate is trusted and has not expired, but there is a mismatch of the name on the DSView software client certificate and the name on the DSView software hub server certificate, a Warning - HTTPS dialog box will appear. Contact the issuer of your certificate.

3. Click *Always* to add the certificate to the Java certificate store.

   If you click *No*, a connection will not be made with the CPS or CCM appliance. If you click *Yes*, a connection will be made with the appliance and the viewer will open, but the warning dialog box will continue to appear each time you connect to the managed appliance.

Managing ActiveX® controls

The DSView management software uses the two following ActiveX controls to provide interactive content:

- Java 1.5.0_02 - Used to display a Telnet Viewer window during a Telnet application or serial session.
- Avocent Video Viewer - Used to display a Video Viewer window during a KVM session.

The functionality of the ActiveX controls is determined by the settings for the security zone being used by the DSView management software. See *Specifying security zones* on page 29 for more information.

To download an ActiveX control on a DSView software hub server using Windows (all operating systems except Windows XP using Service Pack 2):

1. From a Unit Views window Action column for a CPS or CCM appliance, click *Serial Session*.

   -or-

   From a Unit Views window, click on the name of a CPS or CCM appliance. *Overview* will automatically be selected, the name of the appliance will appear at the top of the side navigation bar and the Overview window will open. Click the *Serial Session* icon or text.

   -or-

   From a Unit Views window Action column for a DS1800 digital switch or DSR switch, click *KVM Session*.

   -or-

   From a Unit Views window, click on the name of a DS1800 digital switch or DSR switch. *Overview* will automatically be selected, the name of the DS1800 digital switch or DSR switch will appear at the top of the side navigation bar and the Overview window will open. Click the *KVM Session* icon or text.

   If this is the first time the ActiveX control has been requested by the DSView management software, an Avocent Session Viewer message box will appear, followed by a Security Warning dialog box.

2. Select *Always trust content from Avocent Huntsville Corporation*.
3. Click *Yes* to download the ActiveX control. When the control has been downloaded, a KVM session will start in a Video Viewer window or a serial session will start in a Telnet Viewer window, depending on the supported action for the managed appliance.

If the required ActiveX control could not be loaded, a red X will appear in the Avocent Session Viewer message box. The ActiveX control may fail to load for one of the following reasons:

- The user did not select Always trust content from Avocent Huntsville Corporation.
- The DSView software client security zone settings are not correct
- The ActiveX control failed to properly install.

To download an ActiveX control on a DSView software hub server using Windows Service Pack 2 (Windows XP only):

1. From a Unit Views window Action column for a CPS or CCM appliance, click *Serial Session*.

   -or-

   From a Unit Views window, click on the name of a CPS or CCM appliance. *Overview* will automatically be selected, the name of the appliance will appear at the top of the side navigation bar and the Overview window will open. Click the *Serial Session* icon or text.

   -or-

   From a Unit Views window Action column for a DS1800 digital switch or DSR switch, click *KVM Session.*

   -or-

   From a Unit Views window, click on the name of a DS1800 digital switch or DSR switch. *Overview* will automatically be selected, the name of the DS1800 digital switch or DSR switch will appear at the top of the side navigation bar and the Overview window will open. Click the *KVM Session* icon or text.

   If this is the first time the ActiveX control has been requested by the DSView management software, an Avocent Session Viewer message box will appear.
2. Click in the top yellow bar. A pop-up menu will appear. Click *Install*. A Security Warning dialog box will appear.
3. Click *Install* to install the ActiveX control.

Specifying security zones

Internet Explorer restricts actions performed by the web browser, based on the security zone membership of the web site being accessed. Each security zone typically has its own security restrictions. The following four security zones are available in Internet Explorer:

- Trusted Sites - Web sites contained in the list of trusted sites.
- Restricted Sites - Web sites contained in the list of restricted sites.
- Local Intranet - Web sites accessed using a host name (for example, https://sun-e2-callisto).
- Internet - All other web sites, including those accessed using standard dot notation (for example, https://10.0.0.1).

By default, the DSView management software operates correctly in the Internet, Local Intranet and Trust Sites security zones when accessing a hub server.

NOTE: A DSView software hub server installed on a PC running the Windows 2003 Server will not operate correctly in the Internet security zone.

The current security zone appears in the lower right corner of the DSView Explorer window.

To ensure that the DSView management software works correctly:

Specify settings for the Local Intranet and Internet security zones. When a DSView software client accesses a hub server using a host name (for example, https://avocent), the Local Intranet security zone will be used. When a client accesses a hub server using a web address with periods (for example, https://www.avocent.com), the Internet security zone will be used.

-or-

Add the DSView software hub server to the Trusted Sites list. The DSView software client will always connect to the hub server using the Trusted Sites security zone. The Trusted Sites zone contains very low security settings and ensures successful communication between the client and the hub server.

To display or change the restrictions of a security zone:

1. From Internet Explorer, select *Tools* - *Internet Options*. The Internet Options dialog box will appear.
2. Click the *Security* tab.
3. Select the security zone you wish to view.
4. Click the *Custom Level* button. The Security Settings dialog box will appear.
5. Ensure that the following security settings are set to Enabled or Prompt. The Active Scripting setting should be set to Enabled.
   - Download Signed ActiveX Controls
   - Run ActiveX Controls and Plug-Ins
   - Launching Programs and Files in an IFRAME
   - Active Scripting
6. Click *OK* to save the settings and close the Security Settings dialog box.
7. Click *OK* to close the Internet Options dialog box.

To add a hub server to the Trusted Sites list:

NOTE: If Trusted Sites security zone settings have been modified from their defaults, ensure that the correct settings required for the DSView software are specified, as indicated above.

1. From Internet Explorer, select *Tools* - *Internet Options*. The Internet Options dialog box will appear.
2. Click the *Security* tab.
3. Select *Trusted Sites*.
4. Click the *Sites* button. The Trusted Sites dialog box will appear.

5. Type the web site address, in standard dot notation (xxx.xxx.xxx.xxx), for the DSView software hub server (for example, https://10.0.0.1).
6. Click *Add*. The web site address will appear in the web sites list box.
7. Ensure that *Require server verification (https:) for all sites in this zone* is selected.
8. Click *OK* to save the settings and close the Trusted Sites dialog box.
9. Click *OK* to close the Internet Options dialog box.

Specifying advanced Internet options

Internet Explorer contains advanced settings that may be specified to enhance use of the DSView software. Changing these settings is not required, but is recommended for optimum results.

To specify advanced Internet options for the DSView software:

1. From Internet Explorer, select *Tools - Internet Options*. The Internet Options dialog box will appear.
2. Click the *Advanced* tab.
3. Select the following settings:
   - Always send URLs as UTF-8
   - Disabled script debugging
   - Play animations in web pages
   - Show pictures
   - Print background colors and images
   - Use SSL 2.0
   - Use SSL 3.0
4. Select Enable Integrated Windows Authentication if the DSView software is using Integrated Windows Authentication. See *Using Integrated Windows Authentication* on page 32 for more information.
5. Uncheck the following settings:
   - Always expand ALT text for images
   - Display a notification about every script error
6. Click *OK* to save the settings and close the dialog box.

Using certificates

The DSView software system uses certificates to provide secure transactions between components and to uniquely identify components in the system.

NOTE: A Security Alert, Warning - Security or Warning - HTTPS dialog box may appear if there are issues with a certificate. See *Correcting certificate security alerts* on page 26 for more information.

Server certificate

A DSView software server certificate is used to:

- Uniquely identify the DSView software server to DSView software clients connecting to the server using web browsers
- Uniquely identify the DSView software server to other DSView software servers in the system and provide for secure transactions between them
- Provide for secure transactions between DSView software clients and the DSView software server

By default, a self-signed certificate that uniquely identifies the server is created when the server is installed. The server certificate may be replaced with a certificate from a Certificate Authority (CA) using the Update DSView Server Certificate Wizard.

Client certificates

DSView software client certificates are used for authentication of client users during log in. To use DSView software client certificates for authentication, a DSView software administrator must first enable certificate authentication. See *Client session information* on page 54 for more information. Once this option is enabled, the DSView software server will prompt the client web browser to send its user certificates.

The DSView software client certificate must first be loaded into the client web browser and be associated with a user account. See *Changing certificates associated with users* on page 156 for more information.

Managed appliance certificates

Certificates are also used for authenticating and authorizing managed appliance sessions when a managed appliance is added in secure mode. See *Adding Units* on page 88 for more information.

Using Integrated Windows Authentication

The DSView management software allows DSView software clients to authenticate against Microsoft Windows NT domain and Microsoft Active Directory external authentication servers using Integrated Windows Authentication. This feature allows Single Sign-On (SSO) and is disabled by default.

NOTE: Integrated Windows Authentication cannot be used if the DSView software server name contains periods (.).

To use Integrated Windows Authentication for authentication, a DSView software administrator must first enable it. See *Client session information* on page 54 for more information.

Using the software through a firewall

In a typical network configuration, as shown in Figure 1.5, the DSView software client is located outside of the firewall and the DSView software server and managed appliances reside inside the firewall. In this case, the firewall must be configured to allow two TCP/IP ports inside the firewall.

One TCP port (default=443) is used for the HTTPS web browser connection between the DSView software client and the DSView software server. The other TCP port (default=1078) is used for the Avocent Proxy Protocol to tunnel video and Telnet traffic. Both ports are configurable.

If you are using the DSView management software through a firewall, we recommend the following:

- Place the DSView software server and all managed appliances within the same firewall Demilitarized Zone (DMZ). If the managed appliances are not in the same DMZ with the DSView software server, you must configure the firewall so all data may pass between the zones using TCP/IP ports 22 (SSH), 3211, 2068, 8192 and 3871. You must also configure the User Datagram Protocol (UDP) port 3211 so it may pass through the firewall for initial network discovery of appliances that do not have an IP address.

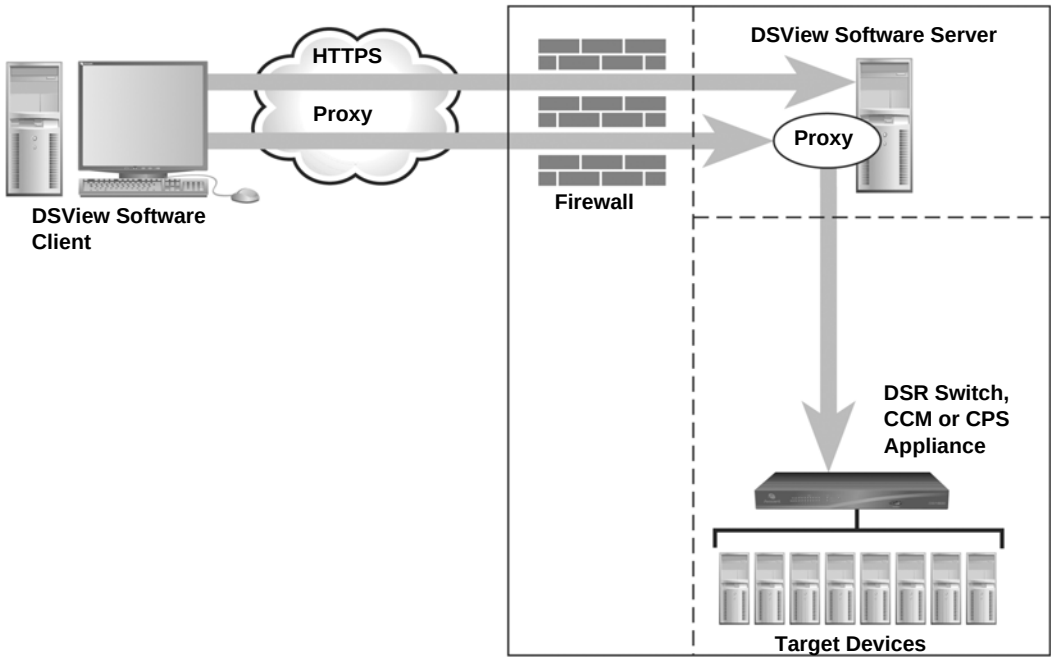


Figure 1.5: Typical DSView Software System Firewall Configuration

Using a VPN

A VPN is a secure network that uses public infrastructure and typically includes several Wide Area Network (WAN) components that may impact performance of the VPN.

Typically, two sites are connected in a VPN network using WANs and a router. This setup provides a secure network between the two sites, but processing is slow.

Several factors related to the network setup, including the DSView software database replication schedule and methods of device access, can affect the speed of a multi-site VPN network. The trade-off must be made based on the network setup.

Frequent replication of the DSView software database will increase WAN/VPN traffic but provide steady data reception at the local sites. Infrequent database replication made at the various sites decreases the WAN/VPN traffic but delays the reception of changes at the local site.

In addition, the methods used to access devices affects network speed. VPN access of a managed appliance is always slower than local access.

The DSView management software supports VPNs that provide full transparency for IP addresses, as well as ports between sites and many VPNs that perform network address translation (NAT) between sites. For example, the VPN in Figure 1.6 could use NAT if Site A and Site B are separate companies that merged but have not resolved their IP addresses. See *Using a NAT device* on page 34 for more information.

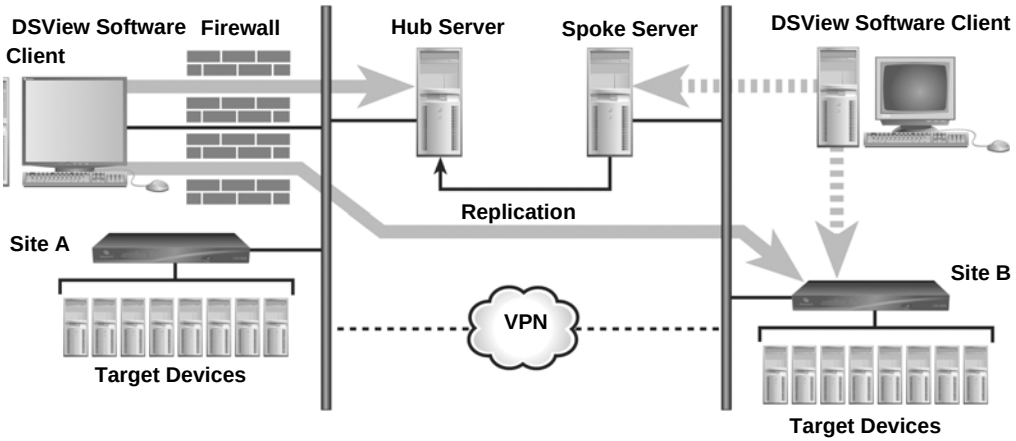


Figure 1.6: DSView Software System on a VPN

Using a NAT device

NAT devices enable a company to use more internal IP addresses than they have assigned to managed appliances. The IP addresses are not exposed outside of the NAT device.

NAT devices are typically used with a DSL broadband router. A DSView software client is connected to the NAT device, as shown in Figure 1.7, which then connects to the corporate network using a VPN.

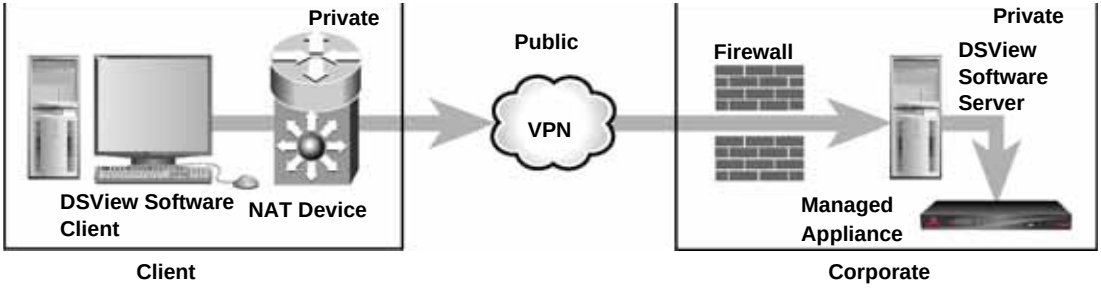


Figure 1.7: Single NAT Configuration (Client Only)

Another scenario, shown in Figure 1.8, is when the corporate site also uses a NAT device to save IP addresses (double-NAT). Since the DSView software client is trying to access a private resource inside the corporate site, the TCP/IP ports used for HTTPS and the proxy server must be configured to be exposed on the corporate NAT device.

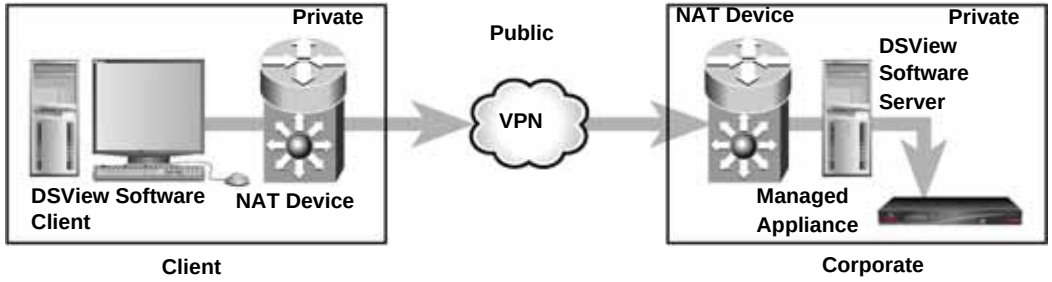


Figure 1.8: Double-NAT Configuration (Client and Corporate)

NOTE: NAT devices may not be connected between the DSView software server and any managed appliances.

CHAPTER 2

Installation

This chapter describes the following installation sequence:

- What you should do before installing the DSView software
- Installing the DSView software
- Configuring the DSView software, plus considerations when upgrading
- Installing the Remote Operations software (if you will be using it)
- Running the DSView software, that is, start a client session

Final sections describe how to change your password, uninstall the software, end a DSView software session and install Java.

About Installation

When the DSView management software is installed, the DSView software database and a hub server are also installed on the dedicated server.

The DSView management software may be installed on a computer containing an existing DSView 2.x software authentication server without causing any interference with the operation of the DSView 2.x software system. The DSView 2.x software authentication server and the DSView management software may run on the same dedicated server at the same time.

Rebooting the dedicated server is not required prior to using the DSView management software.

Once the DSView management software is installed and you have configured the hub server, users may log in at another computer as a DSView software client, using a supported web browser.

You may also install the DSView management software on additional computers and configure them as spoke servers. See *Managing Spoke Servers* on page 73 and *Running the DSView Management Software* on page 45.

NOTE: A license key permits the operation of the DSView software on the dedicated server. The license key also specifies the number of clients that may use the software and the number of spoke servers allowed on a system. Contact your Avocent sales representative for more information about licenses.

Before installing the DSView software

Before installing the DSView management software:

- Install the managed appliance hardware.
- Access the mouse settings on each server connected to a DS1800 digital switch, DSI5100, CPS or CCM appliance or DSR switch and set mouse acceleration to Slow or None.

Minimum requirements for the DSView software

The following are the minimum requirements for installing the DSView management software on a dedicated server or a computer that will function as a DSView software spoke server:

- 1GHz Pentium 3 (2GHz Pentium 4 recommended)
- 512 MB of RAM (1GByte recommended)
- 100BaseT NIC (1GByte LAN recommended)
- 1GB of free disk space
- One of the following operating systems:
  - Microsoft Windows NT® Server
  - Microsoft Windows 2000 Server or Windows 2000 Advanced Server with the latest service package
  - Microsoft Windows Server 2003 Standard, Enterprise and Web Edition
  - Microsoft Windows XP Professional with Service Pack 2 or later
  - Red Hat Enterprise Linux, Version 3 or 4 (AS, ES and WS products)

Installing the DSView Management Software

The DSView management software may be installed using the DSView management software CD or by downloading the software in a self-extracting .zip file from the Avocent web site.

To install the DSView software on a supported Windows system:

1. Log on to the dedicated server as Administrator.
2. To install from a CD:
   a. Insert the DSView software CD. An autorun file will bring up a menu of installation options.
   b. Click *Install DSView Software*.

      -or-

      If autorun is not enabled, type **<drive:>\DSView\win32\setup.exe**, where <drive:> is the letter of your CD-ROM drive.
   c. A dialog box will indicate that the server will be verified to ensure it meets the minimum requirements for installing the DSView software.

   To install from a downloaded file:

   a. Using your web browser, download the DSView management software from the Avocent web site. Go to www.avocent.com and click the *Support* link. On the Technical Support page, click the *Product Upgrades* link, then select *DS Software Upgrades*.

b. Double-click on the downloaded installation package (setup.exe).

c. A dialog box will indicate that the server will be verified to ensure it meets the minimum requirements for installing the DSView management software.

3. If the current or an earlier version of the DSView software is already installed, the Installed Product Found: Same Version message box will appear.

   Click *OK* to reinstall the DSView management software.

   -or-

   Click *Cancel* to exit setup.

4. The Check for an UPDATED version window will open.

   (If the DSView software is already installed on the dedicated server, a message box will display. Click *OK* to close the message box.)

   Click *Next* in the Check for UPDATED Version window to reinstall the software, or click *Cancel* to stop the reinstallation.

   Click *Check for UPDATES* and then click *Next* to check the Avocent web site for the most recent DSView software installation package. Continue to step 5.

   -or-

   Click *Next* to install the CD or downloaded version of the DSView software. Continue to step 6.

5. If a newer version of the DSView software is found, an Update Available message box will appear.

   a. Click *OK* to download the latest DSView software installation package. The installation will be cancelled and the dedicated server's default web browser will launch and open in the Product Upgrades and Options page of the Avocent web site.

      -or-

      Click *Cancel* to resume installation of the older version of the DSView software. Go to step 6.

   b. Type your email address and password and click *Submit* to log in to the web site.

   c. Download the DSView software installation package, log out and close the web browser. Return to step 2.

6. The Introduction window will open. Click *Next*.

7. The License Agreement window will open.

   Click *I accept the terms of the License Agreement* and then click *Next*. Continue to step 8.

   -or-

   Click *I do NOT accept the terms of the License Agreement*. A License Agreement Warning message box will appear. If you click *Quit*, the installation will exit without installing the DSView management software. If you click *Resume*, you will be returned to the License Agreement window.

The DSView management software license agreement may also be viewed from the User Login window by clicking the *Avocent DSView End User License Agreement* link. The agreement will appear in a separate web browser window.

8. If the default TCP port used by the dedicated server hosting the DSView software (TCP port 443) is not available, the Define Web Application Server TCP port window will open.

   Type the port you want to use in the TCP port # field, then click *Next*. (Clicking *Cancel* exits the Checking for an Updated version installation program.)

9. If the default TCP port used by the Avocent proxy server (TCP port 1078) is not available, the Define TD (target device) Session Viewer Proxy TCP port window will open.

   Type the port you want to use in the TCP port # field, then click *Next*.

10. The Choose Destination Location window will open.

    a. Click *Choose* and use the Browse for Folder dialog box to select a directory in which to install the DSView software.

       -or-

       Click *Restore Default Folder* to restore the installation directory to the default (C:\Program Files\Avocent DSView 3).

    b. Click *Install* when you are finished.

    The Installing... window will open and display the progress of the installation. The software will be installed in the specified folder, a Start - *Programs* - *DSView 3.0* shortcut menu will be generated and the DSView management software service startup will be verified. You may cancel the installation by clicking *Cancel*.

    If a previous version of the DSView management software already exists on the dedicated server, message boxes may appear, prompting you to confirm overwriting existing files. Click *Yes to All*.

11. When the software has finished installing, the Successful Service Startup message box will appear. Click *Continue*.

12. The Installation Complete window will open.

    Click *Done* to begin configuration of the DSView software.

    A Security Alert dialog box will appear containing certificate information and a warning that the generator of the certificate is not trusted. This occurs because the DSView software server certificate created when the server is installed is a self-signed certificate. You may either import the certificate into the DSView software client web browser (choosing to trust the certificate) or obtain a server certificate from a Certificate Authority (CA) trusted by the web browser.

    -or-

    Click the *X* (Cancel*)* button in the top right corner of the window to configure the DSView management software at a later time by launching the software from the *Start* menu.

To install the DSView software on a supported Linux system:

1. Log in to the server as root.
2. Insert the DSView software CD into your CD-ROM drive. If AutoMount is supported and enabled, open a command window and continue with step 2.
   -or-
   If your system does not support AutoMount, issue the following command to mount the CD volume:

   mount <device> <mount point>

   Where <device> and <mount point> are the names of your server's CD and mount point, respectively.

   For example, to mount a CD which is the second IDE unit on /media/cdrom, enter the command: `mount /dev/cdrom /media/cdrom`
3. Enter the following command to access the readme file.

   less /media/cdrom/DSView/linux/readme
4. Follow the instructions in the readme file.

Configuring the DSView Management Software

After the DSView software has been installed, it must be configured using a web browser. During the installation process, you are given the choice of launching the web browser or quitting the installation and configuring the software at a later time.

When you initially configure the DSView software installation, a Security Alert dialog box will appear and prompt you to verify that the certificate on the dedicated system is valid before you may proceed. During configuration, you specify whether the computer will be a hub server or a spoke server.

NOTE: If this is your first DSView software server installation, *hub* should be selected in the Select DSView Server Role window. The hub server should be installed before any spoke servers are added.

If the computer will be a hub server, you will need the license key obtained from Avocent and provide a username and password to use for initial log in.

If the computer will be a spoke server, you will need to identify the associated hub server and provide the name/password of the hub server's DSView software administrator.

To configure the DSView management software:

1. If you are configuring the DSView management software during the installation process, click *Done* in the Launch Default Browser window.

   -or-

   If you quit the DSView management software installation process before configuring the software, select *Start - Programs - Avocent DSView 3 - DSView Software*.

A security alert box will appear containing certificate information. See *Using certificates* on page 31 for more information.

The DSView Explorer will open with the Welcome page of the DSView Server Configuration Wizard.

Click *Next*.

2. The Select DSView Server Role window opens.

   Click *Hub* to assign the dedicated server as the hub server, then click *Next*. Continue to step 3.

   -or-

   Click *Spoke* to assign the dedicated server as a spoke server, then click *Next*. Continue to step 8.

3. The Type in Master License Key window opens. Type the Avocent-provided license key for the DSView software hub server, then click *Next*. (DSView management software license keys prior to version 3.0 are not valid.)

   If you did not receive a license key, click the *http://www.avocent.com/activation* link to obtain a license key.

   If the entered license is already in use on another dedicated server, you will receive a license violation when you log in, and you must then configure the server as a spoke server.

4. The Type in Initial Administrator Account window opens. Type a username, a password and confirm the password of the user to whom you wish to give administrator privileges. Usernames are case sensitive and may contain up to 64 characters. Click *Next*.

5. The Updating hub Configuration window will open with the message *Request In Progress Please Wait*. The license key will be installed and a DSView software administrator account will be created. The built-in user groups will also be created.

6. The Completed Successful window will open when configuration is completed. Click *Finish*.

7. The User Login window will open in the DSView Explorer.

You may now log in using the username and password specified during configuration.

If you chose to configure the server as a spoke server in the Select DSView Server Role window or if you entered a duplicate software license key in the Type in Master License Key window, continue with the following steps.

NOTE: The DSView management software versions of the spoke server and the hub server must match in order to register the spoke server. For example, you may not register a spoke server running DSView management software version 3.0 with a hub server running DSView management software 3.1.

8. The Type in Hub Server Address and Port window will open. Type the address of the DSView software hub server using standard dot notation (xxx.xxx.xxx.xxx) or type the DNS name in the Address field. Click *Next*.

9. The Accept DSView Server Certificate window will open. Click *Next* to accept the certificate.

10. The Type in Hub Administrator Credentials window will open. Type a valid username and password for a user with DSView software administrator privileges on the DSView software hub server. Click *Next*.
11. The Registering Spoke Server window will open with the message *Request In Progress Please Wait*. The configuration of the spoke server will be saved to the database of the hub server and the spoke server's certificates will be installed on the hub server.
12. The Completed Successful window will open when the spoke server has been added. Click *Finish*.

Upgrading the DSView software

When upgrading to a newer version of the DSView management software, it is recommended that all DSView software servers are upgraded at the same time. The DSView software hub server should be upgraded first, followed by each spoke server.

A backup of the hub server should be created prior to and after upgrading the hub server. See *Manually Backing up and Restoring Hub Servers* on page 55 for more information.

Installing the DSR Remote Operations Software (Optional)

If your DSView software system includes DSR1021, 1022, 1024, 1020, 1030, 1031, 2020, 2030, 2035, 4020, 4030, 8020, 8030 or 8035 switches, you may use the DSR Remote Operations software for switch access using a dial-up point to point protocol (PPP) modem connection when an Ethernet connection is unavailable.

The DSR Remote Operations software plus its online help and the JRE (Java Runtime Environment will be installed. See *DSR Remote Operations Software* on page 301 for more information.

Minimum requirements for the DSR Remote Operations software

The following are the minimum requirements for installing the DSR Remote Operations software as a DSView software client:

- 650 MHz Pentium or equivalent processor
- 256 MB RAM minimum (256 MB recommended)
- XGA video with graphics accelerator
- Desktop size setting of at least 800 x 600
- Color palette of at least 256 colors
- One of the following operating systems:
    - Windows NT 4.0 Workstation or Server with Service Pack 6a or later
    - Windows 2000 Workstation or Server with Service Pack 2 or later
    - Windows XP Home Edition or Professional

The DSR Remote Operations software is installed from the DSView Management Software CD.

To install the DSR Remote Operations software:

1. Log on to the host system as Administrator.
2. Insert the DSView Management software CD. An autorun file will bring up a menu of installation options.
3. Click *Install DSR Remote Operations*.

   -or-

   If autorun is not enabled, type **<drive:>\DSR Remote Operations\win32\setup.exe**, where <drive:> is the letter of your CD-ROM drive.
4. An installation preparation dialog box displays and the installation program will verify that the client computer meets the minimum requirements for installing the DSR Remote Operations Software.
5. The Introduction window will open. Click *Next*.
6. The License Agreement window will open.

   Click *I accept the terms of the License Agreement* and then click *Next*. Continue to step 7.

   -or-

   Click *I do NOT accept the terms of the License Agreement*. A License Agreement Warning message box will appear. If you click *Quit*, the installation will exit without installing the DSR Remote Operations software. If you click *Resume*, you will be returned to the License Agreement window.
7. The Choose Destination Location window will open.
   a. Click *Choose* and use the Browse for Folder dialog box to select a directory in which to install the DSR Remote Operations software.

      -or-

      Click *Restore Default Folder* to restore the installation directory to the default (C:\Program Files\Avocent DSView 3\DSR Remote Operations).
   b. Click *Next* when you are finished.
8. The Installing... window will open and displays the progress of the installation. The software will be installed in the specified folder and a Start - Programs - Avocent DSView 3.0 - DSR Remote Operations shortcut menu will be created. You may cancel the installation by clicking *Cancel*.

   If a previous version of the DSR Remote Operations software already exists on the Client computer, message boxes may appear asking if you want to overwrite existing files. Click *Yes to All*.
9. When the software has finished installing, the DSR Remote Operations Installation window will open.
   a. If you wish to start the DSR Remote Operations, select *Click here to invoke the DSR Remote Operations application*.
   b. Click *Done* when you are finished.

Running the DSView Management Software

DSView software clients access the DSView management software host using a web browser. Any software required by the client, such as applets and the Java Runtime Environment (JRE), will be automatically installed by the DSView software server host.

The DSView management software uses Secure Sockets Layers (SSL) encryption to send data between the DSView management software host and the web browser on the client to ensure data integrity and privacy. When a user attempts to log in to a DSView software client session, the authentication service configured in the DSView software by the DSView software administrator verifies the credentials of the user. Security alerts related to the certificates on the DSView software host may appear. The DSView software may also use certificates from a third party Certificate Authority (CA), your own internal CA or Public Key Infrastructure (PKI). See *Using certificates* on page 31 for more information.

The following are the minimum requirements for a DSView software client:

- 650 MHz Pentium or equivalent processor
- 256 MB of RAM
- 10 or 100BaseT NIC (100 recommended)
- XGA video with graphics accelerator
- Desktop size setting of at least 800 x 600
- Color palette of at least 256 colors
- One of the following operating systems:
  - Windows NT 4.0 Workstation, Server or Terminal Server with Service Pack 6a or later
  - Windows 2000 Workstation, Server or Terminal Server with Service Pack 2 or later
  - Windows XP Home Edition or Professional
  - Windows 2003 Server Standard, Enterprise or Web Edition
  - Red Hat Enterprise Linux (WS v3, AS v3, ES v3; kernel version 2.4.21)
- One of the following browsers:
  - Internet Explorer 6.0 SP1 or later web browser (Windows operating systems only)
  - Mozilla version 1.7.3 and later
  - Firefox version 1.0 and later
  - Netscape version 7.2 and later

  If you are using Mozilla, Firefox or Netscape, the Video Viewer and the Telnet Viewer clients require Java; see *Java Installation* on page 47 for more information.

Before opening a client session

- Enable cookies and JavaScript on the client's web browser.
- Configure the web browser. If you are using Internet Explorer, see *Configuring Internet Explorer* on page 26 for more information.

To open a client session:

NOTE: If DSView Software Client Certificate Authentication or DSView Software Client Integrated Windows Authentication is being used, the user will not be required to log in. See *Using certificates* on page 31 for more information.

1. From the DSView software client web browser, enter the URL of the server host in the address bar in the format:

   https://<servername>/dsview

   In this case, <servername> is the IP address of the host system, in standard dot notation (xxx.xxx.xxx.xxx) or the DNS name.

   -or-

   If you are opening the session on the DSView software server, you may also select *Start - Programs - Avocent DSView 3 - DSView Software*.
2. Accept all security alerts that may appear as the client computer connects to the DSView software server. The DSView Explorer User Login window will open.
3. Type a valid username and password in the fields provided.

   Depending on the settings specified by the administrator, you may be required to change your password before being allowed to complete the login process. See *Adding User Accounts* on page 153 for more information.
4. Click *Login*. The window that appears depends on the rights assigned to the DSView user that is logging in.

If the client machine uses an onboard video controller and experiences video problems, be sure the BIOS is updated to the latest version.

Uninstalling the DSView Management Software

To uninstall the DSView software on a supported Windows system:

1. Select *Start - Settings - Control Panel*. The Control Panel will appear.
2. From the Control Panel, click *Add/Remove Programs*. The Add/Remove Programs dialog box will appear.
3. Select *Avocent DSView 3.0* and then click *Change/Remove*. The Uninstall Avocent DSView window will open.
4. Click *Uninstall*.

To uninstall the DSView software on a supported Linux system:

1. Log in to the server as root.
2. Insert the DSView software CD into your CD-ROM drive. If AutoMount is supported and enabled, open a command window and continue with step 3.

   -or-

If your system does not support AutoMount, issue the following command to mount the CD volume:

mount <device> <mount point>

Where <device> and <mount point> are the names of your server's CD and mount point, respectively.

For example, to mount a CD which is the second IDE unit on /media/cdrom, enter the command: `mount /dev/cdrom /media/cdrom`

3. Enter the following command to access the readme file.

   less /media/cdrom/DSView/linux/readme

Follow the instructions in the readme file.

Ending a DSView Software Session

To end a DSView software session:

From the DSView Explorer, click *LOGOUT* or the logout icon.

NOTE: Files are copied to DSView software clients when you log in to the DSView software. When using Internet Explorer, temporary files may be removed by selecting the *Delete Temporary Internet Files* command and active web components may be uninstalled by selecting the *Remove Objects* command. See the Internet Explorer documentation for more information.

Java Installation

The Video Viewer and the Telnet Viewer clients require Java when launched from the Mozilla, Netscape or Firefox browsers. The supported Java version is 1.5.0_02. The Telnet Viewer may work with other versions; the Video Viewer requires that version.

The DSView software client automatically downloads and installs the JRE (Java Runtime Environment) the first time the Video Viewer or Telnet Viewer is launched.

On a Windows client, it is recommended that the JRE be installed in the C:\Program Files\ location. If your system automatically installs programs in another location, you may not be able to launch the Video Viewer. In this case, you should access the Java Web Start console, select *File - Preferences - Java*, and then set the installed location of the JVM (Java Virtual Machine).

Only one version of the JRE can be installed in the browser for DSView software support.

Depending on your system's configuration, you may have to log in as the root user to install the JRE. See your system administrator if you need assistance.

To install on a Windows client without JRE previously installed:

1. From a Units View window, click an Action link that will launch the Telnet Viewer or the Video Viewer.
2. A window will open, containing a link for downloading the JRE installer. Download the JRE installer, then close all browser windows.

3. Click on the JRE icon to launch the installer.
4. Restart the browser, and click an Action link that will launch the Telnet Viewer or the Video Viewer.
    - If you chose a Telnet or Serial Session Action link, the Telnet Viewer will launch immediately.
    - If you chose a KVM Session Action link, Java Web Start is launched and will download its own JRE for running the Video Viewer. (This registers the JRE with Web Start; it does not install the JRE a second time.)

To install on a Windows client with JRE previously installed:

From a Units View window, click an Action link that will launch the Telnet Viewer or the Video Viewer.

- If you chose a Telnet or Serial Session Action link, the Telnet Viewer will launch immediately.
- If you chose a KVM Session Action link, Java Web Start is launched and will download its own JRE for running the Video Viewer. (This step registers the existing JRE with Web Start; it does not install another JRE.)

To install on a Red Hat Enterprise Linux client:

1. From a Units View window, click an Action link that will launch the Telnet Viewer or the Video Viewer.
2. A window will open, containing a link for downloading the JRE installer. Download the JRE installer, then close all browser windows.
3. Run the installer.
4. Restart the browser, and click an Action link.
    - If you chose a Telnet or Serial Session Action link, the Telnet Viewer will launch immediately.
    - If you chose a KVM Session Action link, Java Web Start is launched and will download its own JRE for running the Video Viewer. (This step registers the JRE with Web Start; it does not install the JRE a second time.)

CHAPTER 3

DSView Software Servers

This chapter describes how to:

- Configure DSView software server properties
- Backup and restore hub servers
- Manage spoke servers
- Manage DSView software licenses

Server Properties

Table 3.1 lists the DSView software server properties.

Table 3.1: Server Properties

Property	Description
Identity	Name of the DSView software server and the server's role (hub or spoke).
Network	IP address (*) and port used by clients to access the server using the HTTPS (SSL) protocol. You may change the port number used for the HTTPS connection.
Certificate	DSView server certificate presented to DSView software client web browsers. When a DSView software client connects to the server host containing the DSView software, a Security Alert dialog box will appear. If the client user clicks *Yes*, the web browser will accept the certificate for the current session and future sessions to that server will display the Security Alert dialog box. If the client user chooses *Install Certificate*, the self-signed certificate will be installed and trusted on the client and future sessions to the server will not display the Security Alert dialog box. You may create a Certificate Signing Request (CSR) that can be submitted to a Certificate Authority (CA) to obtain a signed server certificate.
Proxy Server	When the Avocent proxy server is used, DSView software client KVM and serial session requests are sent through the DSView software server rather than directly to the DS1800 digital switch, CPS or CCM appliance or DSR switch, which prevents the exposure of the internal address of the managed appliance. You may change the proxy server configuration. EVR1500 environmental monitor, DSI5100 IPMI and generic appliance sessions are not sent through the DSView software server, even when the proxy is enabled.

Table 3.1: Server Properties (Continued)

Property	Description
Trap Destinations	The DSView software server polls DS1800 digital switches, DSI5100, CPS and CCM appliances and DSR switches to determine if they are responding. If the managed appliance does not respond, the DSView software server sends an SNMP Loss Of Communication (LCM) trap or alert to the external SNMP manager. When the DSView software server detects that the appliance is once again communicating, a Regained Communication (RCM) trap is sent from the DSView software server. When a response change occurs during communication between the DSView software server and a managed appliance, the DSView software writes the event to the event log and sends an SNMP trap to the configured trap destinations. Trap destinations may also be specified by clicking on a managed appliance and changing the SNMP appliance settings.
DSView Client Sessions	Settings for inactivity time-out, Single Sign-On (SSO) for the session or restrictions to use specific IP addresses to start the sessions.
Email	IP address of the SMTP (Simple Mail Transfer Protocol) server that is used by the DSView software to send email notifications.
Unit Status Polling	Enables/disables unit status polling for the DSView software server, and specifies the delay between polling cycles and the number of managed appliances that will be concurrently polled.
Spoke Servers	Enables you to manage the DSView software spoke servers in your system.

* When the DSView software server is running on a Linux system, the IP address field may contain the loopback address. If this is not desired, edit the /etc/hosts file on the Linux system. Add a new line above the line that defines the loopback address. The new line should contain the IP address, followed by the host name. For example, the following new line adds the IP address 172.30.20.206 for the host name sun-jcv - fc3.avocent.com, above the existing line that defines the loopback address (127.0.0.1).

```
172.30.20.206    sun-jcv-fc3.avocent.com
127.0.0.1        localhost.localdomain sun-jcv-fc3.avocent.com localhost sun-jcv-fc3
```

To display server properties:

Click the *System* tab. *DSView Server* will automatically be selected in the top navigation bar and *Identity* will automatically be selected in the side navigation bar. The DSView Server Identity Properties window will open. The top of the side navigation bar will indicate the name of the DSView software server.

To change server network properties:

1. Click *Network* in the side navigation bar. The DSView Server Network Properties window will open.
2. Type a new DSView software server port number in the HTTPS Port field.

   If the default value (443) is modified, the port number in the URL must be specified when accessing the DSView software. For example, if the IP address of the hub server is 10.0.0.1

and the port number is changed to 444, **https://10.0.0.1:444/dsview** must be typed in the Address field of the web browser to access the DSView software.

The selected port must be available on the DSView software server. If DSView software clients are located on an external connection, the specified port must be open on the firewall.

3. Click *Save*. A confirmation dialog box will appear.

   A web browser error message will appear when *Save* is clicked. This error message is a normal occurrence. To reestablish connection to the DSView software, you must reconnect to the hub server by typing the URL with the new port number. For example, if you changed the port number to 334 for a hub server with an IP address of 10.0.0.1, type **https://10.0.0.1:334/dsview** to access the DSView management software.

4. Click *Yes* to change the HTTPS port number.

   -or-

   Click *No* to cancel the action.

Certificates

To create a CSR:

NOTE: Certificates may only be viewed by DSView software administrators. See *Using certificates* on page 31 for more information.

1. Click *Certificate* in the side navigation bar. The DSView Server Certificate Properties window will open.
2. Click *Get CSR*. A File Download dialog box will appear.
3. Click *Open*. The CSR is downloaded and displays in the configured text editor.

   -or-

   Click *Save*. The Save As dialog box will appear. Select a directory and filename and click *Save* to save the CSR.

   -or-

   Click *Cancel* to cancel the action.

4. Submit the CSR generated request to a Certificate Authority (CA) to obtain a signed server certificate.
5. Update the DSView software server to use the certificate created by the CA (see next procedure).

To update a certificate on the DSView software server:

NOTE: Certificates may only be viewed by DSView software administrators.

1. Click *Certificate* in the side navigation bar. The DSView Server Certificate Properties window will appear.
2. Click *Update*. The Update DSView Server Certificate Wizard will appear. Click *Next*.

3. The Select Operation to Perform window will open.
4. Select *Create a new self-signed SSL server certificate* to create a minimal security SSL certificate without incurring the costs and overhead involved with a Certificate Authority (CA). Continue to step 5.

   -or-

   Select *Import a signed SSL server certificate* to import a more secure SSL certificate that has been approved (perhaps by a CA). The public key of the imported certificate must match the public key in the certificate that the DSView software server is currently using. This requires that both certificates be made on the same DSView software server. Continue to step 6.

   Click *Next*.
5. The Type in Certificate Information window will open.
   a. Type the name of the computer that will serve as the DSView software server on your intranet in the Common Name field.

      -or-

      If the DSView software server is outside the intranet, type the server's full domain name in dot notation format (xxx.xxx.xxx.xxx).
   b. Type the name of the organization (or country).
   c. Type the name of the organizational division or name under which the organization is doing business.
   d. Type the complete city or location name. The City or Location field is required for organizations registered only at the local level.
   e. Type the complete name of the state or province where the organization is located.
   f. Type the two-character ISO country code for the country where the organization is located.
   g. Click *Next*. Go to step 7.
6. The Select Certificate to Import window will open.
   a. Type the full directory and filename for the SSL certificate file you wish to import to the DSView software server.

      -or-

      Click the *Browse* button and specify the SSL certificate file.

      The name of the SSL certificate file must be entered in case sensitive text if your operating system supports case sensitive filenames.

      Imported certificates must have been generated from a CSR created on the same DSView software Server to which you are importing the certificate.
   b. Click *Next*.
7. The Completed Successful window will open.

8. Click *Finish*. The DSView Server Certificate Properties window will open containing updated certificate information.

Proxy servers

To specify a proxy server:

NOTE: This procedure is valid for the following managed appliances: DS1800 digital switches, CPS appliances, CCM appliances and DSR switches.

1. Click *Proxy Server* in the side navigation bar. The DSView Server Proxy Properties window will open.
   a. Type a new port number to use for DSView software client communication with the Avocent proxy to the logged in DSView software server.

NOTE: If DSView software clients are located on an external connection, the specified TCP/IP proxy port must be opened on your firewall.

   b. Select the type of Proxy Invocation:
      - Click *Disable the proxy server* to allow all internal and external DSView software clients to communicate directly with the managed appliances. (This is the default.)
      - Click *Use the proxy server for all KVM, serial and virtual media sessions* to enable all DSView Clients to communicate with the managed appliances using the DSView software proxy server.
      - Click *Use the proxy server only for clients not on the same network as this DSView Server* to enable all external and internal clients on a different network than the current DSView software server to communicate with the managed appliances using the DSView proxy server. All other external and internal clients will communicate directly with the managed appliances.
      - Click *Use the proxy server only for clients connecting with the following addresses* to enable only DSView software clients with IP addresses entered in the Address List to communicate with the managed appliances using the DSView proxy server. All other clients communicate directly with the managed appliances.

NOTE: Changing the Proxy Port or Proxy Invocation setting will disconnect active DSView software client sessions.

2. Click *Save*. A confirmation dialog box will appear.
3. Click *OK* to save your changes.

   -or-

   Click *Cancel* to cancel the action.

Server trap destinations

To specify trap destinations:

1. Click *Trap Destinations* in the side navigation bar. The DSView Server Trap Destinations window will open.
2. In each address field, type the IP addresses in standard dot notation (xxx.xxx.xxx.xxx) or the domain name for the computer that handles traps. Up to four computers may be specified.
3. Click *Save* to store the trap information in the DSView software database on the host.

Client session information

To specify client session information:

1. Click *DSView Client Sessions* in the side navigation bar. The DSView Server Client Session Properties window will open.
   a. Use the arrows to specify a time-out value (from 5-60 minutes) for inactivity of a DSView user client session. The default is 15 minutes. When the time-out value has been exceeded, the session will end and the user must log in again.
   b. Select *Enable certificate authentication* to allow the DSView management software to automatically log in internal users if the user certificate (X.509 digital ID) installed in the DSView software client web browser matches the certificate configured for the user. Certificates for users may be modified. See *Changing certificates associated with users* on page 156 for more information.

      Web browser settings may need to be modified to allow users to automatically log in using certificates. See your web browser documentation for more information.

      -or-

      Select *Enable Integrated Windows® Authentication* to automatically log a user into the DSView management software using the user's NT domain or Active Directory credentials and Integrated Windows Authentication.

      Web browser settings may need to be modified to allow users to automatically log in using Integrated Windows Authentication. See your web browser documentation for more information.
   c. Select *Restrict by address range* to enable only DSView software clients with IP addresses entered in the Address List to communicate with DS1800 digital switches, CPS appliances, CCM appliances and DSR switches.

      -or-

      Do not select *Restrict by address range* to disable address restrictions for logging into the DSView management software.
2. Click *Save* to store client session information in the DSView software database on the host.

Email

To specify email properties:

1. Click *Email* in the side navigation bar. The DSView Server Email Server Properties window will open.
2. Type a new address for the SMTP server that sends email notifications as a domain name or an IP address in standard dot notation (xxx.xxx.xxx.xxx).
3. If your SMTP server requires login credentials, select *Login required to access SMTP server* and type a user name and password, then confirm the password.
4. Click *Save* to store DSView software email property information in the DSView software database on the host.

Unit status polling

To use unit status polling:

1. Click *Unit Status Polling* in the side navigation bar. The DSView Server Unit Status Polling Properties window will open.
2. Select *Enable unit status polling*.
3. Type the number of seconds to wait between polling cycles (from 30-999 seconds). The default is 900 seconds (15 minutes). A smaller value results in greater accuracy.
4. Type the number of managed appliances that may simultaneously be polled to obtain status information (from 1-25 units). The default is 5. A larger number results in faster speed.
5. Click *Save* to store unit status property information in the DSView software database on the host.

Manually Backing up and Restoring Hub Servers

NOTE: You may only restore a DSView software hub server with a backup archive made using an identical DSView management software version. For example, you may not restore a hub server running DSView management software version 3.1 using a backup archive made with DSView management software 3.0.

You may manually create a backup of your hub server. Two methods are available:

- From a command line in an MS-DOS window. This method may be used for DSView software hub servers on supported Windows or Linux systems.
- Using the Backup and Restore Utility delivered with the DSView software. The backup is saved as a .zip file containing the files needed to restore the DSView management software. This method may be used for DSView software hub servers on supported Windows systems only.

Client sessions will be temporarily disconnected during a manual backup. The sessions will be automatically reconnected when the backup is completed.

Hub server backups may also be automatically created as a task within the DSView software. If you use the Backup DSView database and system files task, client sessions will not be temporarily disconnected. See *Managing Tasks* on page 255 for more information.

To manually backup or restore a hub server using a command line on a supported Windows system:

NOTE: This procedure requires DSView software administrator privileges.

1. In the Start menu on your desktop, select *Start - Programs - Accessories - Command Prompt*. A command prompt window will open.
2. Change directories to the directory in which the DSView software is installed (typically C:\Program Files\Avocent DSView 3.0\bin).
3. Enter **DSViewBackupRestore** to display the DSView 3.0 Backup/Restore Utility dialog box. Follow the directions in *To manually back up a DSView software hub server using the Backup and Restore Utility dialog box* to back up the DSView software hub server using the dialog box or *To manually restore a DSView software hub server using the Backup and Restore Utility dialog box* to restore the DSView software hub server using the dialog box.

   -or-

   To backup the DSView software hub server, enter **DSViewBackupRestore -backup -archive "<archive name>" -passwd <password>**.

   -or-

   To restore the DSView software hub server, enter **DSViewBackupRestore -restore -archive "<archive name>" -passwd <password>**.

   "<archive name>" - Name of the archive, which must be enclosed by quotation marks (for example, "myarchive"). The -archive option and an archive name are required.

   <password> - A password that encrypts the archive. The password is optional when creating a backup. If a password is specified when creating the backup, it will be required when restoring the backup.

   To display help information, type **DSViewBackupRestore -h** or **DSViewBackupRestore -help**.

For example, entering the following in a command prompt window will create a backup named db.zip with the password test.

```
DSViewBackupRestore.exe -backup -archive "db.zip" -passwd test
```

Entering the following in a command prompt window will restore a backup named db.zip with the password test.

```
DSViewBackupRestore.exe -restore -archive "db.zip" -passwd test
```

To manually backup or restore a hub server using a command line on a supported Linux system:

1. Access the command prompt on your system.

2. Change directories to the directory where the DSView software is installed, which is typically /usr/local/dsviewserver/bin.
3. To backup the DSView software hub server, enter **DSViewBackupRestore.sh -backup -archive <archive name> -passwd <password> -overwrite**.
4. To restore the DSView software hub server, enter **DSViewBackupRestore.sh -restore -archive <archive name> -passwd <password>**.

   <archive name> - Name of the archive. The -archive option and an archive name are required.

   <password> - A password that encrypts the archive. The password is optional when creating a backup. If a password is specified when creating the backup, it will be required when restoring the backup.

   -overwrite - Enables overwriting of an existing archive during backup. If this parameter is omitted, no overwriting will occur.

   To display help information, type **DSViewBackupRestore.sh -help**.

For example, entering the following in a command prompt window will create a backup named dbasebackup.zip with the password test1.

```
DSViewBackupRestore.sh backup -archive dbasebackup.zip -passwd test1
```

Entering the following in a command prompt window will restore a backup named dbasebackup.zip with the password test.

```
DSViewBackupRestore.sh restore -archive dbasebackup.zip -passwd test1
```

To manually back up a hub server using the Backup and Restore Utility dialog box on a supported Windows system:

NOTE: This procedure requires DSView software administrator privileges.

1. In the Start menu on your desktop, select *Start - Programs - Avocent DSView 3 - Backup and Restore Utility*. The DSView 3 Backup/Restore Utility dialog box will appear.
2. Click *Backup Database to a file.*
3. If you wish to password-protect the backup file, click *Enabled* and type a password in the Password field.
4. Click *Browse* and use the Save As dialog box to specify a directory and name for the backup file. Click *Save* when you are finished.
5. Click *Backup*. The DSView software system backup files are saved.
6. Click *Close* to close the DSView 3 Backup/Restore Utility dialog box.

To manually restore a hub server using the Backup and Restore Utility on a supported Windows system:

1. In the Start menu on your desktop, select *Start - Programs - Avocent DSView 3.0 - Backup and Restore Utility*. The DSView 3 Backup/Restore Utility dialog box will appear.

2. From the DSView 3 Backup/Restore Utility dialog box, click *Restore the database from a file*.
3. If the backup file is password-protected, click *Enabled* and type its password in the Password field.
4. Click *Browse* and use the Save As dialog box to find the backup file.
5. Click *Restore*. The DSView software system is restored from the backup files.
6. Click *Close* to close the DSView 3.0 Backup/Restore Utility dialog box.

Managing Authentication Services

Users must be authenticated before they may access or perform any tasks in the DSView management software system.

When users log in, they will be prompted for a username and password. The DSView software will look up the login, determine the authentication service to use and forward the login credentials to the appropriate authentication service for verification. All authentication is performed over an HTTPS (SSL) encrypted link.

NOTE: Some web browsers may store password information. See your web browser documentation for more information.

The DSView software is delivered with the DSView internal authentication service, which verifies a log in and password against user account information stored in the database on the DSView software server.

The DSView software also supports the following external authentication services:

- Microsoft Active Directory® *
- IBM® SecureWay® Directory Server *
- Novell® LDAP Services *
- Sun® Solaris™ R9 LDAP Directory Server *
- Sun ONE™ LDAP Directory Server *
- Microsoft Windows NT domain
- Cisco® Secure ACS 3.3 for Windows 2000/2003 server
- Microsoft IAS for Windows 2000/2003 server
- FreeRADIUS for Red Hat RHL3
- Cisco Secure ACS 3.3 for Windows 2000/2003 server

* Uses LDAP V3

If the DSView software server is configured for external authentication, login requests are re-directed to the configured external authentication server.

NOTE: The DSView software obtains external group membership and external user information when a user logs in. If a user's group membership changes or the user is deleted externally, the DSView software will not see these changes until the next time the user logs in.

The User Authentication Services window may be customized by using the *Customize* link. See *Using the Customize link in windows* on page 15 for more information.

You may schedule a task that will automatically verify LDAP and Active Directory external authentication servers to ensure that accounts are still valid. See *Managing Tasks* on page 255 for more information.

To display configured authentication services:

1. Click the *Users* tab.
2. Click *Authentication Services* in the top navigation bar. The User Authentication Services window will open.

To add an Active Directory external authentication service:

NOTE: Only User Administrators and DSView software administrators may add authentication services.

1. In the User Authentication Services window, click *Add*. The welcome window of the Add Authentication Service Wizard will appear. Click *Next*.
2. The Provide Authentication Service Name and Type window will open.
   a. Type a name for the external authentication service.
   b. Select *Active Directory* from the drop-down menu.
   c. Click *Next*.
3. The Specify Active Directory Connection Settings window will open.
   a. Type the Active Directory domain name for the domain you wish to add in the AD Domain Name field.
   b. In the User Container field, specify the name of the container to search for user accounts. This will limit the search scope to that container. The name may be entered in several forms, optionally including a sub-domain. Valid forms are explained below by example.

      Assume an Active Directory domain name of “sunrise.mycompany.com” with users in subfolder “sun/myusers.” The User Container field may be entered as:

      Example 1 (no sub-domain): “sun.myusers”

      Example 2 (no sub-domain): “ou=myusers,ou=sun”

      If users are contained in a sub-domain such as “mktg.sunrise.mycompany.com”, valid forms are:

      Example 1 (with sub-domain): “mktg.sunrise.mycompany.com/sun/myusers”

      Example 1 (with sub-domain and no container specified): “mktg.sunrise.mycompnay.com/”

      Example 2 (with sub-domain): “ou=myusers,ou=sun,dc=mktg,dc=sunrise,dc=mycompany,dc=com”

c. In the Group Container field, specify the name of the container to search for user groups. This will limit the search scope to that container. The name may be entered in several forms, optionally including a sub-domain. Valid forms are explained in step 3b above.

d. In the Username Type drop-down menu, select the type of username. Each choice in the menu contains an example.

A Full Windows 2000 username is specified as username@domain.
A Partial Windows 2000 username is specified as username.
A Full Pre-Windows 2000 username is specified as domain\username.
A Partial Pre-Windows 2000 username is specified as username.

This option may only be configured for new authentication servers; it cannot be modified. Existing authentication servers are set to the Partial Windows 2000 Username type for compatibility.

e. Specify a Secure Socket Layer (SSL) encryption mode:

- Click *Do Not Use SSL* to have authentication performed using unencrypted clear text instead of SSL encryption. This method is the least secure.
- Click *Use SSL in Trust All Mode* to use SSL encryption for data transmission. All server certificates will be trusted and automatically accepted by the DSView software for transmitting data. This SSL method provides medium security.

  This encryption mode is not recommended for wide area networks (WANs).
- Click *Use SSL in Certificate-based Trust Mode* to use SSL encryption for data transmission. The DSView management software will approve the server and then the certificate before transmitting data. This SSL method provides maximum security.

f. Click *Use Kerberos for User Authentication* to use the Kerberos protocol for authentication requests, including the browsing. If enabled, you must use DES encryption types for this account. If an account was created prior to Active Directory, the user's password must be changed after this setting is changed. In addition, the Active Directory server addresses must be resolvable to their host names via DNS.

When this is not checked, the LDAP protocol will be used.

g. Click *Enable Chasing of Referrals* to allow the Active Directory server to refer DSView software clients to additional directory servers.

h. Click *Use an Active Directory Global Catalog* to have the AD service access the global catalog for the specified domain name.

i. Click *Next*.

If you selected *Use SSL in Certificate-based Trust Mode*, continue to step 4.

If you selected *Do Not Use SSL* or *Use SSL in Trust All Mode*, go to step 6.

4. The Accept Certificate window will open and list all servers that belong to the domain.
5. Click *Next* to accept the certificate.
6. The Select Browsing Method window will open.

Click *Browse Anonymously* to browse users on the external Active Directory authentication server.

-or-

Click *Browse with user credentials* to browse users on the external Active Directory authentication based on credentials configured on the server. If this option is selected, do the following:

a. Type the username for an Active Directory account that has browse rights in the User Name field. The login ID must be entered in case sensitive text if the Active Directory server is set up to use Kerberos. When using Kerberos, the browse account cannot be specified in the Full Pre-Windows 2000 Username form (domain\username). If the username is in a sub-domain of the Active Directory domain (specified in step 3a), then the username should be specified as <username>@<subdomain>.

b. Type the password for an Active Directory account that has browse rights in the Password field.

c. Click *Next*.

7. The Establish Connection with Authentication Service window will open briefly. If the external authentication service is added successfully, the Completed Successful window will open.
8. Click *Finish*. The User Authentication Services window will open with the new service listed.

To add a Windows NT external authentication service:

1. In the User Authentication Services window, click *Add*. The Add Authentication Service Wizard will appear. Click *Next*.
2. The Provide Authentication Service Name and Type window will open.
   a. Type a name for the external authentication service.
   b. Select *Windows NT Domain* from the drop-down menu.
   c. Click *Next*.
3. The Specify Windows NT Connection Settings window will open. Type the Windows NT domain name you wish to add in the Domain Name field, and then click *Next*.
4. The Select Browsing Method window will open.

   Click *Browse Anonymously* to browse users on the external Windows NT authentication server.

   -or-

   Click *Browse with user credentials* to browse users on the external Windows NT authentication based on credentials configured on the server. If this option is selected, do the following:

   a. Type the username for a Windows NT account that has browse rights in the User Name field.

b. Type the password for a Windows NT account that has browse rights in the Password field.

c. Click *Next*.

5. The Establish Connection with Authentication Service window will briefly appear. If the external authentication service is added successfully, the Completed Successful window will open.

6. Click *Finish*. The User Authentication Services window will open with the new service listed.

To add an LDAP external authentication service:

1. In the User Authentication Services window, click *Add*. The Add Authentication Service Wizard will appear. Click *Next*.

2. The Provide Authentication Service Name and Type window will open.

   a. Type a name for the external authentication service.

   b. Select *LDAP* from the Type drop-down menu.

   c. Click *Next*.

3. The Specify LDAP Connection Settings window will open.

   a. Type the address of the LDAP host in dot notation format (xxx.xxx.xxx.xxx) or type the DNS host name in the Host Address field.

   b. Type the number of the port for connecting to the LDAP host in the Port Number field.

   c. Specify an SSL encryption mode:

      - Click *Do Not Use SSL* to have authentication performed using unencrypted clear text instead of SSL encryption. This method is the least secure and automatically sets the Port Number field to a default port number of 389.
      - Click *Use SSL in Trust All Mode* to use SSL encryption for data transmission. All server certificates will be trusted and automatically accepted by the DSView software for transmitting data. This SSL method provides medium security and automatically sets the Port Number field to a default port number of 636.

        This encryption mode is not recommended for wide area networks (WANs).
      - Click *Use SSL in Certificate-based Trust Mode* to use SSL encryption for data transmission. The DSView 0software will approve the server and then the certificate before transmitting data. This SSL method provides maximum security and automatically sets the Port Number field to a default port number of 636.

   d. Click *Enable Chasing of Referrals* if you wish to allow the LDAP server to refer DSView software clients to additional directory servers.

   e. Click *Next*.

   If you selected *Use SSL in Certificate-based Trust Mode*, continue to step 4.

   If you selected *Do Not Use SSL* or *Use SSL in Trust All Mode*, go to step 8.

4. The Accept Certificate window will open and list all servers that belong to the domain.

5. Click *Next* to accept the certificate.
6. The Specify LDAP User Schema window will open.
   a. Type the Base distinguished name (DN) from which to begin searches. This is a required field unless the Directory Service has been configured to allow anonymous search. Each Search DN value must be separated by a comma.
   b. Type the key attribute. The default value is common name (cn).
   c. Type the object class. The default value is person.
   d. Type the full name attribute. The default value is surname (sn).
   e. Click *Next*.
7. The Specify LDAP Group Schema window will open.
   a. Type the Base distinguished name (DN) from which to begin searches. This is a required field unless the Directory Service has been configured to allow anonymous search. Each Search DN value must be separated by a comma.
   b. Type the object class. The default value is group.
   c. Type the member attribute. The default value is member.
   d. Click *Next*.
8. The Select Browsing Method window will open.

   Click *Browse Anonymously* to browse users on the external LDAP authentication server.

   -or-

   Click *Browse with user credentials* to browse users on the external LDAP authentication based on credentials configured on the server. If this option is selected, do the following:
   a. Type a log in ID in the User Name field, in one of two forms: a fully qualified distinguished name or the username of an account in the base user DN.
   b. Type the password for the LDAP user account in the Password field.
   c. Click *Next*.
9. The Establish Connection with Authentication Service window will open briefly. If the external authentication service is added successfully, the Completed Successful window will open.
10. Click *Finish*. The User Authentication Services window will open with the new service listed.

To add a RADIUS external authentication service:

1. On the RADIUS server that will be used as an external authentication service, add the DSView software server as a RADIUS client. Make a note of the configured shared secret and the available authentication type(s) on the RADIUS server.
2. From the DSView Explorer, in the User Authentication Services window, click *Add*. The Add Authentication Service Wizard will appear. Click *Next*.
3. The Provide Authentication Service Name and Type window will open.

a. Type a 1-64 character name for the RADIUS authentication service.
b. Select *RADIUS* from the Type drop-down menu.
c. Click *Next*.

4. The Specify RADIUS Connection Settings window will open.
   a. Type the address of the RADIUS host in dot notation format (xxx.xxx.xxx.xxx) or type the DNS host name in the Server Address field.
   b. Type the number of the port (from 1-65535) for connecting to the RADIUS host in the Port Number field. The default is port 1812.
   c. Click *Next*.
5. The Establish Connection with Authentication Service window will open briefly. If the external authentication service is contacted successfully, the Specify RADIUS Authentication Settings window will open.
   a. Select the authentication type from the Authentication Type drop-down menu. Make sure it is one of the available authentication types noted in step 1.

      PAP - Password Authentication Protocol
      CHAP - Challenge Handshake Authentication Protocol (default)
      MS-CHAP - Microsoft Challenge Handshake Authentication Protocol
      MS-CHAP v2 - Microsoft Challenge Handshake Authentication Protocol Version 2

   b. In the Shared Secret field, type the shared secret (that was configured on the RADIUS server in step 1), which is a password protected field. Microsoft's implementation allows up to 128 ASCII characters for the shared secret; other servers may have a different limit.
   c. Reenter the shared secret in the Confirm Shared Secret field.
   d. Click *Next*.
6. If the external authentication service is added successfully, the Completed Successful window will open.
7. Click *Finish*. The User Authentication Services window will open with the new service listed.

To add a TACACS+ external authentication service:

1. On the TACACS+ server that will be used as an external authentication service, add the DSView software server as a TACACS+ client. Make a note of the configured shared secret and the available authentication type(s) on the TACACS+ server.
2. In the User Authentication Services window, click *Add*. The Add Authentication Service Wizard will appear. Click *Next*.
3. The Provide Authentication Service Name and Type window will open.
   a. Type a 1-64 character name for the TACACS+ authentication service.
   b. Select *TACACS+* from the Type drop-down menu.
   c. Click *Next*.
4. The Specify TACACS+ Connection Settings window will open.

a. Type the address of the TACACS+ host in dot notation format (xxx.xxx.xxx.xxx) or type the DNS host name in the Server Address field.

b. Type the number of the port (from 1-65535) connecting to the TACACS+ host in the Port Number field. The default is port 49.

c. Click *Next*.

5. The Establish Connection with Authentication Service window will open briefly. If the external authentication service is contacted successfully, the Specify TACACS+ Authentication Settings window will open.

   a. Select the authentication type from the Authentication Type drop-down menu. Make sure it is one of the available authentication types noted in step 1.

      PAP - Password Authentication Protocol
      CHAP - Challenge Handshake Authentication Protocol (default)
      MS-CHAP - Microsoft Challenge Handshake Authentication Protocol

   b. In the Shared Secret field, type the shared secret (that was configured on the TACACS+ server in step 1), which is a password protected field. Microsoft's implementation allows up to 128 ASCII characters for the shared secret; other servers may have a different limit.

   c. Reenter the shared secret in the Confirm Shared Secret field.

   d. Click *Next*.

6. If the external authentication service is added successfully, the Completed Successful window will open.

7. Click *Finish*. The User Authentication Services window will open with the new service listed.

To change the DSView internal authentication service account policies:

NOTE: Only user administrators and DSView software administrators may change authentication services.

1. In the User Authentication Services window, click *DSView Internal*. The side navigation bar will change to include DSView Internal at the top and, below the name, the information you may define.

2. Click *Account Policies*. The Authentication Service User Account Policies - DSView Internal window will open.

3. Specify the password policies for the authentication service:

   a. Type a number (from 1-64) in the Minimum Password Length field, or click the arrows to select a number.

   b. Check the *Passwords Expire* checkbox if you wish to require a user to change their password after a certain amount of time. Specify the time by typing a number (from 1-365) in the Maximum Expiration (days) field, or click the arrows to select a number.

   c. Select *Passwords must contain both alpha and numeric characters* if new passwords must contain at least one letter and one number.

d. Select *Passwords must contain both lower and upper case characters* if new passwords must contain at least one uppercase and one lowercase letter.

4. Specify the lockout policy for the authentication service:
   a. Select *Lockout users after invalid login attempts* to assign a specific number of user login attempts. Continue to step b.

      -or-

      Leave the checkbox unselected to specify unlimited user login attempts. Go to step 6.

   b. Type the number of allowable user login failures (from 1-25) in the Maximum Login Failures field, or select it using the drop-down menu.

   c. Select *Automatically unlock users after the lockout period* to permit user logins after a certain amount of time. Specify the lockout period (in minutes) by typing a number (from 1-1,440) in the Maximum Lockout Period (minutes) field, or select it using the drop-down menu. Specifying 1,440 minutes is equivalent to 24 hours.

      -or-

      Leave the checkbox unselected if you do not wish to specify a lockout period. If you do not specify a lockout period, a user administrator or administrator must manually unlock locked user accounts. See *Unlocking User Accounts* on page 155 for more information.

5. Click *Save* and then click *Close*. The User Authentication Services window will open.

To change custom field labels for user accounts that use internal authentication:

1. In the User Authentication Service window, click *DSView Internal*. The side navigation bar will change to include DSView Internal at the top and, below the name, information you may define.
2. Click *Custom Field Labels* in the side navigation bar. The Authentication Service User Account Custom Field Labels - DSView Internal window will open.
3. Type the text that you wish to appear in each of the six custom field labels.
4. Click *Save* and then click *Close*. The User Authentication Services window will open.

By default, the custom field labels do not display in the User Accounts - All window, but they may be added to the display, using the Customize link. See *Using the Customize link in windows* on page 15 for more information.

To change connections for Windows NT external authentication services:

1. In the User Authentication Services window, click the name of the Windows NT service. The side navigation bar will change to include the name of the service at the top and, below the name, the information you may define.
2. Click *Connection* in the side navigation bar. The Authentication Service Connection Settings - NT window will open.
3. Type a name in the Service Name field to change the name of the service that appears in the Name column of the User Authentication Services window.

4. Type the name of the Windows NT domain in the Domain Name field.
5. Click *Save* and then click *Close*. The User Authentication Services window will open.

To change user browsing settings for Windows NT external authentication services:

1. In the User Authentication Services window, click the name of the Windows NT service. The side navigation bar will change to include the name of the Windows NT service at the top and, below the name, the information you may define.
2. Click *User Browsing* in the side navigation bar. The Authentication Service User Browsing - NT window will open.
3. Click *Browse Anonymously* to anonymously browse users on the external Windows NT authentication server.

   -or-

   Click *Browse with User Credentials* to browse users on the external Windows NT authentication based on credentials configured. If this option is selected, do the following:

   a. Type the username for an NT domain account that has browse rights in the User Name field.
   b. Type the password for an NT domain account that has browse rights in the Password field.
4. Click *Save* and then click *Close*. The User Authentication Services dialog box will appear.

To change settings for Active Directory external authentication services:

1. In the User Authentication Services window, click the name of the Active Directory (AD) service. The side navigation bar will change to include the name of the AD service at the top and, below the name, the information you may define.
2. Click *Connection* in the side navigation bar. The Authentication Service Connection Settings - AD window will open.
3. Type a name in the Service Name field to change the name of the service that appears in the Name column of the User Authentication Services window.
4. Type the domain name of the Active Directory service in the AD Domain Name field.
5. In the User Container field, specify the name of the container to search for user accounts. This will limit the search scope to that container. The name may be entered in several forms, optionally including a sub-domain. See *To add an Active Directory external authentication service:* on page 59 for an explanation of the valid forms.
6. In the Group Container field, specify the name of the container to search for user groups. This will limit the search scope to that container. The name may be entered in several forms, optionally including a sub-domain. See *To add an Active Directory external authentication service:* on page 59 for an explanation of the valid forms.
7. Specify a Secure Socket Layer (SSL) Encryption mode:

- Click *Do Not Use SSL* to have authentication performed using unencrypted clear text instead of SSL encryption. This method is the least secure.
- Click *Use SSL in Trust All Mode* to use SSL encryption for data transmission. All server certificates will be trusted and automatically accepted by the DSView management software for transmitting data. This SSL method provides medium security.

  This encryption mode is not recommended for wide area networks (WANs).
- Click *Use SSL in Certificate-based Trust Mode* to use SSL encryption for data transmission. The DSView management software will approve the server and then the certificate before transmitting data. This SSL method provides maximum security.

8. Click *Use an Active Directory Global Catalog* to have the AD service access the global catalog for the specified domain name.
9. Click *Use Kerberos for User Authentication* to use the Kerberos protocol for authentication requests, including the browsing. If enabled, you must use DES encryption types for this account. If an account was created prior to Active Directory, the user's password must be changed after this setting is changed. In addition, the Active Directory server addresses must be resolvable to their host names via DNS.

   When this is not checked, the LDAP protocol will be used.
10. Click *Save* to save your changes.

    If you selected *Use SSL in Certificate-based Trust Mode*, the Certificates heading will appear in the side navigation bar. Continue to step 11.

    -or-

    If you selected *Do Not Use SSL* or *Use SSL in Trust All Mode*, go to step 14.
11. Click *Certificates*. The Authentication Service Certificate Management - AD window will open and list all servers that in the domain.
12. To register certificates:
    a. To select one or more certificates, click the checkbox to the left of the server IP addresses.

       -or-

       To select all certificates, click the checkbox to the left of the IP Address heading.
    b. Click the *Register* button above the IP Address list to register the certificates. The Accept SSL Certificate window will open.
    c. Click *Save* to store the certificate values to the DSView software database on the host.

       -or-

       Click *Close* if you do not wish to save the certificate values.

       The Authentication Service Certificate Management window will open if only one certificate was selected. If more than one certificate was selected, each will appear in order in subsequent Accept SSL Certificate windows.
13. To unregister certificates:
    a. To select one or more certificates, click the checkbox to the left of the server IP addresses.

-or-

b. To unregister all certificates, click the checkbox to the left of the IP Address heading.

c. Click the *Unregister* button to unregister the certificates.

d. A confirmation message box will appear. Click *OK* to unregister the server.

-or-

Click *Cancel* to cancel the action.

14. Click *Close*. The User Authentication Services window will open.

To change user browsing settings for Active Directory external authentication services:

1. In the User Authentication Services window, click the name of the AD service. The side navigation bar will change to include the name of the AD service at the top and, below the name, the information you may define.
2. From the side navigation bar, click *User Browsing*. The Authentication Service User Browsing - AD window will open.
3. Click *Browse Anonymously* to browse users on the external Active Directory authentication server.

   -or-

   Click *Browse with User Credentials* to browse users on the external Active Directory authentication based on credentials configured on the server. If this option is selected, do the following:

   a. Type the username for an Active Directory account that has browse rights in the User Name field. The log in ID must be entered in case sensitive text if the Active Directory server is set up to use Kerberos.

   b. Type the password for an Active Directory account that has browse rights in the Password field.

4. Click *Save* and then click *Close*. The User Authentication Services dialog box will appear.

To change connections for LDAP external authentication services:

1. In the User Authentication Services window, click the name of the LDAP service. The side navigation bar will change to include the name of the LDAP service at the top and, below the name, the information you may define.
2. Click *Connection* in the side navigation bar. The Authentication Service Connection Settings - LDAP window will open.
3. Type a name in the Service Name field to change the name of the service that appears in the Name column of the User Authentication Services window.
4. Type the address of the LDAP host, in dot notation format (xxx.xxx.xxx.xxx) in the Host Address field.

5. Type the number of the port you with to use for connecting to the LDAP host in the Port Number field.
6. Specify a Secure Socket Layer (SSL) Encryption mode:
   - Click *Do Not Use SSL* to have authentication performed using unencrypted clear text instead of SSL encryption. This method is the least secure and automatically sets the Port Number field to a default port number of 389.
   - Click *Use SSL in Trust All Mode* to use SSL encryption for data transmission. All server certificates will be trusted and automatically accepted by the DSView management software for transmitting data. This SSL method provides medium security and automatically sets the Port Number field to a default port number of 636.

     This encryption mode is not recommended for wide area networks (WANs).
   - Click *Use SSL in Certificate-based Trust Mode* to use SSL encryption for data transmission. The DSView management software will approve the server and then the certificate before transmitting data. This SSL method provides maximum security and automatically sets the Port Number field to a default port number of 636.
7. Click *Save* to save your changes.

   If you selected *Use SSL in Certificate-based Trust Mode*, the Certificates heading will appear in the side navigation bar. Continue to step 8.

   -or-

   If you selected *Do Not Use SSL* or *Use SSL in Trust All Mode*, go to step 15.
8. Click *Certificates*. The Authentication Service Certificate Management - LDAP window will open and list all servers that belong to the domain.
9. To register certificates, click the checkbox to the left of the server IP address(es).

   -or-

   Click the checkbox to the left of the IP Address heading to select all server IP addresses listed in the window.
10. Click the *Register* button to register the certificates. The Accept SSL Certificate window will appear.
11. Click *Save* to store the certificate values to the DSView software database on the host.

    -or-

    Click *Close* if you do not wish to save the certificate values.

    The Certificate Management window will open if only one certificate was selected. If more than one certificate was selected, each will appear in order in subsequent Accept SSL Certificate windows.
12. To unregister certificates, click the checkbox to the left of the server IP address(es).

    -or-

    Click the checkbox to the left of the IP Address heading to select all server IP addresses listed in the window.

13. Click the *Unregister* button to unregister the certificates.
14. A confirmation message box will appear. Click *OK* to confirm or *Cancel* to cancel.
15. Click *Close*. The User Authentication Services window will open.

To change user schema settings for LDAP external authentication services:

1. In the User Authentication Services window, click the name of the LDAP service. The side navigation bar will change to include the name of the LDAP service at the top and, below the name, the information you may define.
2. Click *Schema* in the side navigation bar. *Users* will automatically be selected and the Authentication Service User Schema - LDAP window will open.
3. Type the Base distinguished name (DN) from which to begin searches. This is a required field unless the Directory Service has been configured to allow anonymous search. Each Search DN value must be separated by a comma.
4. Type the key attribute. The default value is common name (cn).
5. Type the object class. The default value is person.
6. Type the full name attribute for the user. The default value is surname (sn).
7. Click *Save* and then click *Close*. The User Authentication Services dialog box will appear.

To change group schema settings for LDAP external authentication services:

1. In the User Authentication Services window, click the name of the LDAP service. The side navigation bar will change to include the name of the LDAP service at the top and, below the name, the information you may define.
2. Click *Schema* in the side navigation bar, and then click *Groups*. The Authentication Service Group Schema - LDAP window will open.
3. Type the Base distinguished name (DN) from which to begin searches. This is a required field unless the Directory Service has been configured to allow anonymous search.
4. Type the object class. The default value is groupOfNames.
5. Type the members attribute. The default value is member.
6. Click *Save* and then click *Close*. The User Authentication Services dialog box will appear.

To change user browsing settings for LDAP external authentication services:

1. In the User Authentication Services window, click the name of the LDAP service. The side navigation bar will change to include the name of the LDAP service at the top and, below the name, the information you may define.
2. Click *User Browsing* in the side navigation bar. The Authentication Service User Browsing - LDAP window will open.
3. Click *Browse Anonymously* to browse users on the external LDAP authentication server.

   -or-

Click *Browse with User Credentials* to browse users on the external LDAP authentication based on credentials configured on the server. If this option is selected, do the following:

a. Type a log in ID in the User Name field, in one of two forms: a fully qualified distinguished name or the username of an account in the base user DN.

b. Type the password for the LDAP user account in the *Password* field.

4. Click *Save* and then click *Close*. The User Authentication Services dialog box will appear.

To change settings for RADIUS external authentication services:

1. In the User Authentication Services window, click the name of the RADIUS service. The side navigation bar will change to include the name of the RADIUS service at the top and, below the name, the information you may define.
2. Click *Connection* in the side navigation bar. The Authentication Service Connection Settings - RADIUS window will open.
   a. Type a 1-64 character name for the RADIUS authentication service.
   b. Type the address of the RADIUS host in dot notation format (xxx.xxx.xxx.xxx) or type the DNS host name in the Server Address field.
   c. Type the number of the port (from 1-65535) for connecting to the RADIUS host in the Port Number field. The default is port 1812.
   d. Click *Save*.
3. To change the authentication type and/or shared secret, click *Settings* in the side navigation bar. The Authentication Service Authentication Settings - RADIUS window will open.
   a. Select the authentication type from the Authentication Type drop-down menu.

      PAP - Password Authentication Protocol
      CHAP - Challenge Handshake Authentication Protocol (default)
      MS-CHAP - Microsoft Challenge Handshake Authentication Protocol
      MS-CHAP v2 - Microsoft Challenge Handshake Authentication Protocol Version 2

   b. In the Shared Secret field, type the shared secret, which is a password protected field. Microsoft's implementation allows up to 128 ASCII characters for the shared secret; other servers may have a different limit.
   c. Reenter the shared secret in the Confirm Shared Secret field.
   d. Click *Save*.
4. Click *Close*. The User Authentication Services dialog box will appear.

To change settings for TACACS+ external authentication services:

1. In the User Authentication Services window, click the name of the TACACS+ service. The side navigation bar will change to include the name of the TACACS+ service at the top and, below the name, the information you may define.
2. Click *Connection* in the side navigation bar. The Authentication Service Connection Settings - TACACS+ window will open.

a. Type a 1-64 character name for the TACACS+ authentication service.
b. Type the address of the TACACS+ host in dot notation format (xxx.xxx.xxx.xxx) or type the DNS host name in the Server Address field.
c. Type the number of the port (from 1-65535) for connecting to the TACACS+ host in the Port Number field. The default is port 49.
d. Click *Save*.

3. To change the authentication type and/or shared secret, click *Settings* in the side navigation bar. The Authentication Service Authentication Settings - TACACS+ window will open.
   a. Select the authentication type from the Authentication Type drop-down menu.

      PAP - Password Authentication Protocol
      CHAP - Challenge Handshake Authentication Protocol (default)
      MS-CHAP - Microsoft Challenge Handshake Authentication Protocol

   b. In the Shared Secret field, type the shared secret, which is a password protected field. (Microsoft's implementation allows up to 128 ASCII characters for the shared secret; other servers may have a different limit.)
   c. Reenter the shared secret in the Confirm Shared Secret field.
   d. Click *Save*.
4. Click *Close*. The User Authentication Services dialog box will appear.

To remove authentication services:

NOTE: Only user administrators and DSView software administrators may remove authentication services. The DSView internal authentication service may not be removed.

1. In the User Authentication Services window, click the checkbox to the left of the authentication service(s) you wish to delete.

   -or-

   Click the checkbox to the left of Name to select all external authentication services listed in the window for deletion.
2. Click *Delete*. A confirmation dialog box will appear.
3. Click *Yes* to confirm or *No* to cancel the action.

Managing Spoke Servers

Information on the hub server is replicated on the spoke server. The spoke server's information, such as its IP address, port number and certificate, is stored in the hub server's database.

You may optionally specify up to 15 computers as spoke servers. Contact your Avocent sales representative for information about spoke server licenses.

NOTE: The DSView management software versions of the spoke server and hub server must match in order to register a spoke server. For example, you may not register a spoke server running DSView management software version 3.0 with a hub server running DSView management software 3.1.

A spoke server may be created by:

- Specifying a spoke server when installing the DSView management software.
- Converting a hub server to a spoke server by registering it as a spoke to another DSView software hub server. The DSView software system data on the hub server being converted will be lost and the converted hub server will replicate the data of the new specified hub server.

You may also change the properties of a spoke server or remove spoke servers from your system.

To display a list of spoke servers:

NOTE: The Spoke Servers window is only available on the hub server.

1. Click the *System* tab.
2. Click *DSView Server* in the top navigation bar. The side navigation bar will include the name of the server to which you are logged in.
3. Click *Properties* in the side navigation bar, and then click *Spoke Servers*. The Spoke Servers window will open.

Each spoke server in the display has a status icon. Table 3.2 lists the possible status values.

Table 3.2: DSView Software Spoke Server Status Icons

Icon	Description	Cause
	Responding	Normal operation. The hub and spoke servers are communicating with each other using HTTPS.
	Not responding	The hub and spoke servers cannot communicate with each other using HTTPS. This typically indicates a network communication error. Ensure that network connectivity is occurring between the two servers.
	Hub/Spoke Versions Not Compatible	The versions of DSView management software on the hub server and spoke servers are not compatible.
	Certificates Do Not Match	Certificates on the hub server and spoke servers do not match. See *Managing hub and spoke server certificates* on page 76 for information about updating the server certificates so that they will match.
	Invalid Server or Versions Not Compatible	A server responded, but it is not compatible with the DSView software. This typically occurs when communication is attempted with a server that does not contain the software, or if either server contains an older version of the software. Ensure that both servers are running the same DSView software version.

You may remove some fields from the display by using the Customize link. See *Using the Customize link in windows* on page 15 for more information.

To add a spoke server:

1. Install the DSView management software on the computer you wish to use as a spoke server. See *Installing the DSView Management Software* on page 38 for more information.
2. Configure the computer as a spoke server. See *Configuring the DSView Management Software* on page 41 for more information.

To register a hub server as a spoke server:

NOTE: Only DSView software administrators may register a hub server as a spoke server.

NOTE: When registering a hub server as a spoke server on another DSView software system, the information on the hub server being registered will be lost. Its database will be updated to match the new hub server to which it is being registered.

1. Click the *System* tab.
2. Click *DSView Server* in the top navigation bar. The side navigation bar will include the name of the server to which you are logged in.
3. Select *Tools* in the side navigation bar. The DSView Server Tools window will open.
4. Click the *Register as Spoke Server* icon or text. The Register Spoke Server Wizard will appear. Click *Next*.
5. The Type in Hub DSView Server Address window will open.
   a. Type the IP address of the hub server in standard dot notation (xxx.xxx.xxx.xxx).

      -or-

      Type the domain name of the hub server.

   b. Type the port number for the hub server.

      If the default hub server port value (443) is modified, you must specify it when registering a spoke server so that register requests will be sent to the correct port on the hub server. For example, if the IP address of the hub server is 10.0.0.1 and the port number is changed to 444, type **https://10.0.0.1:444/dsview** in the Address field of the Register Spoke Server Wizard.
6. Click *Next*.
7. The Operation in Progress window will open briefly, followed by the Accept Hub DSView Server Certificate window. Click *Next*.
8. The Type in Hub DSView Server Administrator Credentials window will open.
9. Click *Next*.
   a. Type the name of a user with DSView software administrator privileges on the hub server.
   b. Type a password for the user.

10. The Operation In Progress window will open with the message *Request In Progress Please Wait*. The configuration of the spoke server will be saved to the database of the hub server and the spoke server's certificates will be installed on the hub server.
11. The Completed Successful window will open when the spoke server has been added.
12. Click *Finish*. The Audit DSView Server Tools window will open.

To change spoke server network properties:

NOTE: Spoke server network settings may need to be modified by DSView software administrators when network settings are changed and the the hub server did not automatically detect the changes. When changing the network settings, ensure that a port mismatch does not occur between the hub server and the spoke server.

1. On the hub server, in the Spoke Servers window, click on the name of the spoke server whose network properties you wish to change. The Spoke Server Network Properties window will open.
2. Change any of the following network settings:
   a. Type a new computer name to use as the spoke server.
   b. Type a new address in standard dot notation (xxx.xxx.xxx.xxx) for the spoke server.
   c. Type a new port number for the spoke server.
3. Click *Save* and then click *Close*. The Spoke Servers window will open.

Managing hub and spoke server certificates

When a spoke server is registered with a hub server, a certificate trust relationship is established between the two servers. Certificate information must match on the hub server and the spoke servers for communication to take place between the servers. If the spoke server certificate is subsequently changed, a certificate mismatch will occur.

To display or update the certificate of a spoke server on the hub server:

NOTE: Certificates may only be viewed by DSView software administrators and user administrators.

1. On the hub server, click the *System* tab. *DSView Server* will automatically be selected in the top navigation bar and the name of the DSView software hub server will appear at the top of the side navigation bar.
2. Click *Spoke Servers* in the side navigation bar. The Spoke Servers window will open.
3. In the Spoke Servers window, click *Certificate*. The Spoke Server Certificate window will open including information about the spoke server certificate (Actual Certificate) and the certificate registered for this spoke server on the hub server (Registered Certificate).
4. The window displays the certificate on the spoke server and the certificate registered on the hub server.

   If the DSView management software cannot obtain the certificate information from the spoke server, a message will appear at the bottom of the DSView Server Certificate - Spoke Server

window. The message states: *Remote server is not responding. Information displayed may not match remote side*.

If the certificate information does not match, continue to step 5.

- or -

If the certificate information matches, go to step 6.

5. Click *Update*. The spoke server certificate information will be updated on the hub server.
6. Click *Close*. The Spoke Servers window will open.

To update the certificate of a hub server on the spoke server:

1. On the spoke server, click the *System* tab. *DSView Server* will automatically be selected in the top navigation bar and the name of the spoke server will appear at the top of the side navigation bar.
2. Click *Hub Server* in the side navigation bar. The Hub Server window will open.
3. In the hub Server window, click *Certificate*. The Hub Server Certificate window will open including information about the spoke server certificate (Actual Certificate) and the certificate registered for this spoke server on the hub server (Registered Certificate).

   If the DSView software cannot obtain the certificate information from the hub server, a message will appear at the bottom of the DSView Server Certificate - Hub Server window. The message states: *Remote server is not responding. Information displayed may not match remote side*.

   If the certificate information does not match, continue to step 4.
4. Click *Update*. The hub server certificate information will be updated on the spoke server.

To delete a spoke server:

1. On the hub server, in the Spoke Servers window, click the checkbox to the left of the spoke servers you wish to delete.

   -or-

   Click the checkbox to the left of Name at the top of the list to select all spoke servers listed in the window for deletion.
2. Click *Delete*. A confirmation dialog box will appear.
3. Click *OK* to confirm or *Cancel* to cancel.

NOTE: When a spoke server is deleted, it is no longer allowed to communicate with the hub server. Only spoke servers that are no longer active should be deleted. If a spoke server is still active, it may be re-registered using the Register Spoke Server wizard.

Replication

Replication is a task that synchronizes the hub and spoke server databases. By default, replication runs every 12 hours on each spoke server. A spoke server's first replication occurs automatically

when the spoke server is added to the DSView software system. You may change the interval that the replication task runs on each spoke server, or you may initiate an immediate replication.

During replication, the spoke server sends all of its database changes since the last replication to the hub server. The hub server then incorporates those changes and sends all of its database changes since the last replication to the spoke server (excluding the changes that spoke server just sent to the hub server).

If an item is added on a spoke server, and another item with the same name (but perhaps with different configuration parameters) is added on the hub server, then after replication, both items will appear on both the hub and spoke servers, with a tilde (~) and a number added to one of the names. The administrator should handle the issue appropriately - in some cases, the duplicate item may need to be renamed; in others, the duplicate item should be deleted.

When different changes are made to one existing item, two outcomes are possible. For example, assume an item is added and configured on the hub server and is then replicated to the spoke server. Later, an administrator changes something about the item on the spoke server. Another administrator then changes something about the item on the hub server. When the replication task runs, two things may happen.

In a few instances where no conflict occurs, both changes will be incorporated and replicated. For example, if the hub server's administrator adds username JaneDoe to the existing user-defined user group Accounting and the spoke server's administrator adds username JohnDoe to the Accounting user group, both names will be added and replicated.

In most other instances where the changes are mutually exclusive or some other conflict occurs, the most recent change will be the only change accepted and replicated. For example, if the hub server's administrator associates a unit with the Miami site, and the spoke server's administrator associates the same unit with the Chicago site, the change that was made closest to the time of replication (that is, the most recent change) will be accepted and replicated.

This emphasizes the importance of ensuring the hub and spoke servers' clocks are synchronized.

The exception to the last-change rule is when one of the actions deletes an item - in that case, the deletion is accepted and replicated, regardless of timing. For example, if a unit was deleted on the hub server, and then the contact information for the same unit was changed on the spoke server a minute later, the unit will be deleted when the replication task is run.

To display replication results and/or change the replication schedule for a spoke server:

1. From the spoke server, click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Select the *Database Replication* task. The Task Results - Database Replication window will open. This window contains the results of the most recent replication.
4. To display or change the replication schedule, click *Schedule* in the side navigation bar. The Task Schedule - Database Replication window will open.

By default, the replication task runs every 12 hours. You may change the schedule type, start time, date and interval.

5. If you change the schedule, click *Save* and then *Close*.

You may also display the replication schedule from the hub server, but you cannot change it.

To initiate an immediate replication on a spoke server:

1. From the spoke server, click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.
3. Enable the checkbox to the left of the Database Replication task and then click *Run Now.*

To display the replication schedule for a spoke server from the hub server:

1. From the hub server, click the *System* tab.
2. Click *Tasks* in the top navigation bar.
3. Select the *Database Replication* task for the spoke server you wish to view. The Task Schedule - Database Replication window will open.

Managing Licenses

License keys permit the operation of the DSView management software on the dedicated server and specify the number of clients that may use the software and the number of spoke servers allowed on a system.

To display license information:

1. Click the *System* tab.
2. Click *Licenses* in the top navigation bar.
3. Click *Summary* in the side navigation bar. The License Summary window will open. The display includes:
   - The serial number of the license key for the DSView software on the dedicated server.
   - The number of licensed clients and the number of users currently logged in as clients. If a site license has been purchased, the Unlimited heading will appear instead of the number of licenses.
   - The total number of licensed spoke servers and the number of these licenses currently in use on the DSView software system.

To display license keys:

1. Click the *System* tab.
2. Click *Licenses* in the top navigation bar.
3. Click *License Keys* in the side navigation bar. The License Keys window will open and list each installed license key and a description of the key. One of the following descriptions will display beside each key:

- Master License Key - The key used when the software was initially installed on the dedicated server.
- Adds <N> Spoke Servers - A key that adds <N> spoke servers.
- Adds <N> Client Session(s) - A key that enables <N> simultaneous DSView software client sessions across all servers.
- Client Session Site License - A key that is installed as a site license, which allows an unlimited number of DSView software client sessions. This will appear for any key that has been purchased as a site license.

To add a new license key:

1. Click the *System* tab.
2. Click *Licenses* in the top navigation bar.
3. Click *License Keys* in the side navigation bar. The License Keys window will open.
4. Click *Add*. The Add Add-On License Key window will open.
5. If you did not receive a license key, click the http://www.avocent.com/activation link to obtain a license key.
6. Type a valid (new 25-character) license key in the License Key field. (License keys from a DSView software release prior to version 3.0 are not valid.)
7. Click *Save*. The License Keys window appears containing the new license key.

   -or-

   Click *Close*. A dialog box will appear and prompt you to save any changes. Click *Yes* to add the license key, or click *No* to cancel the action. The License Keys window will open and contain the license key if you saved the changes.

CHAPTER 4

Managing Units

From the Units windows, you may:

- Add, delete, change and scan units
- Add access rights to units
- Export units or the rights associated with them
- Group units by site, department, location, unit or custom fields

About Unit Views

Only the units for which the user has been assigned privileges will display in the content area. Units will also not display if they are hidden. See *Showing and hiding units* on page 83 for more information.

For information about using the collapse/expand icons in the side navigation bar, see *Using the side navigation bar* on page 12.

To display managed appliances in an Appliances window:

1. Click *Units* in the tab bar. *Units* will automatically be selected in the top navigation bar.
2. Click *Appliances* in the side navigation bar. The Appliances - All window will open.
3. Click on one of the managed appliance links in the side navigation bar to display the Appliances window you wish to view.

Managed appliances that you have recently accessed may also be displayed by clicking *Recently Accessed* under Unit Views in the side navigation bar.

An appliance type will only be listed in the side navigation bar if an appliance of that type has been added to the DSView software system (and the user has access to it). For example, if no DSR1021 switch, CPS810 appliance or EVR1500 environmental monitor exists on your DSView software system, these types will not appear under Appliances in the side navigation bar

To display target devices in a Target Devices window:

Click *Units* in the tab bar. *Units* will automatically be selected in the top navigation bar and *Unit Views - Target Devices - All* will automatically be selected in the side navigation bar. The Target Devices - All window will open, listing all target devices on your system.

Target device types are defined by users. If a type has been assigned to a target device, the type name will appear under Target Devices in the side navigation bar. For example, if you assign a type of Windows 2000 program to three target devices, a Windows 2000 link will appear in the side navigation bar. Clicking on the link will display the three target devices, as well as any other existing target devices assigned that type.

Topology view

The Topology window lists all units, cascade switches, SPC devices and outlets in a hierarchal tree form. Units are arranged in a parent-child hierarchy, with children (target devices) tiered under their parent managed appliance. An SPC power control device will appear as a cascade device attached to a CPS or CCM appliance or DSR switch that supports SPC devices. Each outlet will appear with a power indicator cascaded below the port.

The following rules apply to the Topology window:

- If a target device is connected to multiple switches or appliances, it will appear multiple times in the Topology window.
- Cascade devices, such as SPC devices and AutoView and OutLook legacy analog KVM switches, may not be modified from the Topology window.
- If the Topology window has been customized to display items using multiple pages, and a parent managed appliance and its children (target devices) cannot be displayed in a single Topology window page, it will be repeated on subsequent pages. A repeated unit will contain (continued...) after its name. If the Items per Page setting has been customized to a number so small that all parents cannot be repeated, only the parent closest to the target device will be repeated.

Scan mode is not available when using the Topology view.

To display units and SPC devices and outlets in the Topology window:

1. Click *Units* in the tab bar. *Units* will automatically be selected in the top navigation bar.
2. Click *Topology* in the side navigation bar. The Topology window will open with a display of all appliances in addition to SPC devices and outlets in your system.

Other side navigation bar links

The side navigation bar also contains the following links that may be used to perform other unit related tasks:

- Clicking *Recently Accessed* displays a list of units that the logged in user has accessed last.
- Clicking *Active Sessions* accesses the Active Sessions window, which may be used to remove or display information about target device sessions. See *Managing Active Sessions* on page 129 for more information.
- Clicking *Custom Field Labels* specifies information for custom fields. See *Managing units by custom fields* on page 144 for more information.
- Clicking *Tools* accesses unit tools. See *Using Unit Tools* on page 243 for more information.

- Clicking a link under *Sites* or a custom field displays a list of appliances associated with the site or custom field. A site or custom field will not appear in the side navigation bar unless at least one site or custom field has been defined, at least one unit is associated with the site or custom field and the user has access to the unit.

Showing and hiding units

Figure 4.1 explains some shown and hidden displays window features.

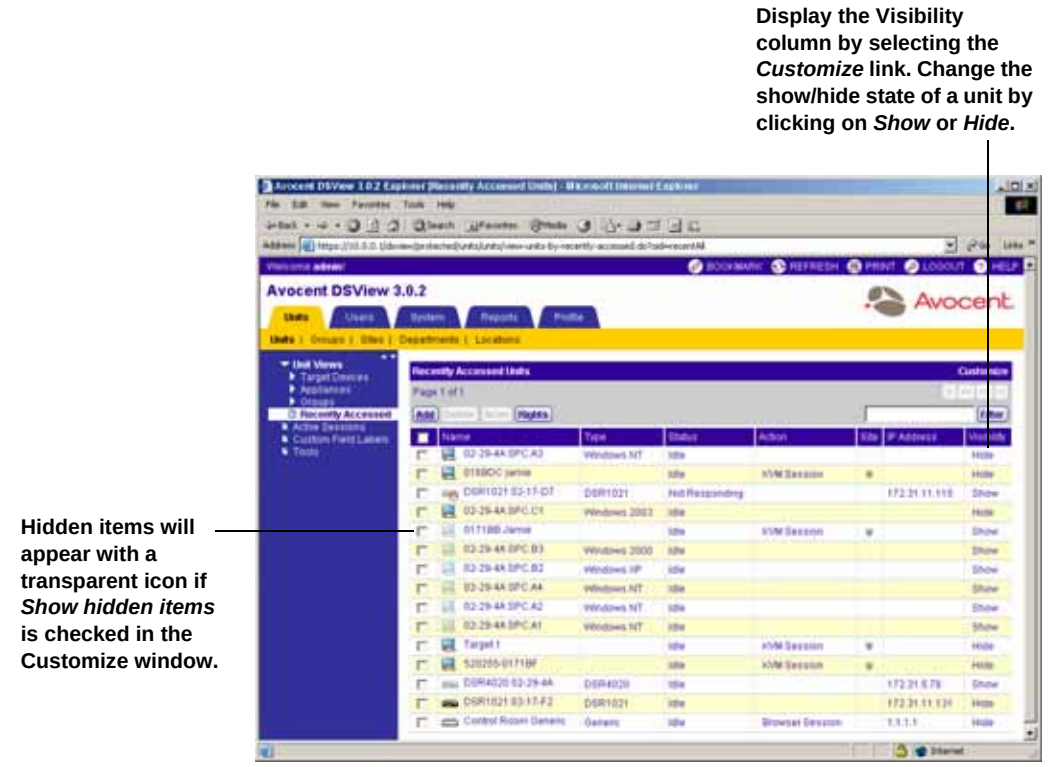

Display the Visibility column by selecting the *Customize* link. Change the show/hide state of a unit by clicking on *Show* or *Hide*.
Hidden items will appear with a transparent icon if *Show hidden items* is checked in the Customize window.
Avocent DSView 3.0.2
Avocent

Figure 4.1: Shown and Hidden Units in a Recently Accessed Units Window

Hiding turns off the display of units in the window, but does not remove the units from your DSView software system.

To hide a unit:

1. Click *Units* in the tab bar. *Units* will automatically be selected in the top navigation bar.
2. Click *Customize* in a Unit Views window. The Unit Views Customization window will open.
3. Click *Visibility* in the Available Fields column and then click *Add*. Visibility will be moved to the Fields to Show column.

4. Click *Show hidden items* if you wish to display hidden units in the Unit Views Customization window with a transparent icon.
5. Click *Save* and then click *Close*. The window will open containing the Visibility column. The Visibility column will display Hide for each unit.
6. Click *Hide* for each unit. The display of the selected unit will be turned off in the Unit Views window if *Show hidden items* was not selected in the Unit Views Customization window.

   -or-

   If *Show hidden items* was selected, the hidden unit will appear with a transparent icon.

To show a hidden unit:

1. Click *Customize* in a Unit Views window. The Unit Views Customization window will open.
2. Click *Visibility* in the Available Fields column and then click *Add*. Visibility will be moved to the Fields to Show column.
3. Click *Show hidden items*.
4. Click *Save* and then click *Close*. The Unit Views window will open containing the hidden items and the Visibility column. Hidden items will have a transparent icon and the Visibility column will display the Show listing.
5. Click *Show*. The selected unit will be made visible, the transparent icon will be changed to a non-transparent icon and the Visibility column will display the Hide listing.

Customizing Unit Views windows

By default, the following fields appear in the Unit Views windows:

- Name - Unit names. You may click on a name to display and change information or specify an icon to associate with a unit. See *Managing Units* on page 95 for information.
- Type - Type of target device or managed appliance model. See *Changing Unit Overview Information* on page 95 for information about assigning a type to a target device.
- Status - Current activity level of a unit. The following status IDs may display for units:
  - Idle - The unit is powered up with no connection.
  - In Use - The unit has at least one active connection.
  - Status Unknown - The status of the unit was reported to the software but cannot be obtained for an unknown reason.

  The following status IDs may display for target devices only:
  - No Power - The target device is powered down.
  - KVM Blocked - The connection path to the target device is blocked because a cascade switch is already in use.
  - Partial Power - The DSView software cannot determine the power state of the target device, or the software received a mixed power state from the target device. For example, if a target device has a KVM connection and an SPC connection, the software will prompt

for a power status for both of these connections. If both connections do not reply with ON or OFF, the power status will display as Partial Power.

The Not Responding status ID may display for managed appliances only. In this case, the managed appliance did not provide status information. This may occur for multiple reasons, such as the appliance is not powered up or it is disconnected from the DSView software system.

An icon appears to the right of the Name column to represent the status of a unit. Figure 4.1 lists and describes the status icons that may appear.

Table 4.1: Unit Status Icons

Icon in Name Field	Description in Status Field	Displays for
	In Use	Units
	Not Responding	Managed Appliances
	No Power	Target Devices
	KVM Blocked	Target Devices
	Partial Power	Target Devices
	Status Unknown	Units

- Action - Type of session that may be initiated. Although an EVR1500 environmental monitor, generic appliance or target device may have multiple actions that may be performed (for example, a target device may be able to open using a browser session and a Telnet session), only one action will appear in the Action column. The action that appears is based on the precedence of the action, which is determined by the software, and whether the action is valid on the unit.

  For example, a target device that is only attached to a CCM appliance will not contain a KVM Session link in a Unit Views window. If a target device has a connection to both a CCM appliance and a DS1800 digital switch or DSR switch, a KVM Session link will appear.

  As shown in Figure 4.2, other available actions may be accessed by clicking the *Alternate Actions* arrow to the right of the action with the highest precedence. Clicking on one of the displayed links will launch the corresponding window type.

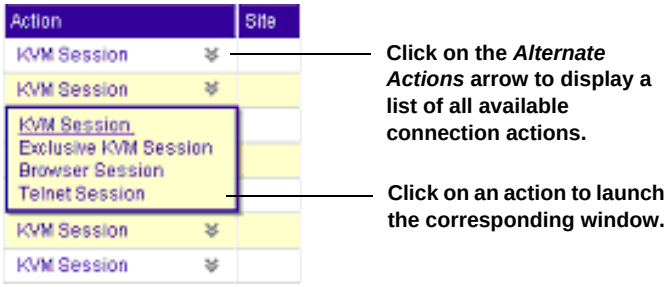


Figure 4.2: Alternate Actions Arrow in a Unit Views Window

Table 4.2 describes the types of sessions (actions) and the precedence of each action.

Table 4.2: Actions to Initiate DSView Software Sessions

Action	Description	From	Precedence
KVM Session	Opens a Video Viewer window session	Target devices	1 (Highest)
Exclusive KVM Session	Opens a Video Viewer window session	Target devices	1*
Virtual Media Session	Opens a Video Viewer window session	Target devices	1
Reserved Virtual Media Session	Opens a Video Viewer window session	Target devices	1*
<name> Embedded Session	Opens a video session	IBM ASM RSA II, DRAC 4 and NEC IPF embedded units	1
IPMI Session	Opens an IPMI Viewer window	IPMI 1.5 target devices	3
Serial Session	Opens a Telnet viewer window session	Target devices	4
Browser Session	Opens a web browser	Target devices, EVR1500 environmental monitors, generic appliances or Compaq iLO embedded units	5
Telnet Session	Opens a Telnet Viewer window session	Target devices, EVR1500 environmental monitors or generic appliances	6

Table 4.2: Actions to Initiate DSView Software Sessions (Continued)

* Exclusive KVM Session or Reserved Virtual Media Session appears in a Unit Views window only when the Alternate Actions arrow is selected in the Action column. An exclusive KVM or reserved virtual media session is shown immediately after its associated KVM or virtual media session. For example, if a target device has two available KVM sessions, clicking the alternate actions icon in the Action column will display KVM Session 1, Exclusive KVM Session 1, KVM Session 2 and Exclusive KVM Session 2.

- Site - Name of a unit site. See *Grouping units by site* on page 135 for more information.

The following fields are not displayed by default, but may be displayed by using the *Customize* link:

- Browser URL - URL that may be used to access a target device, EVR1500 environmental monitor or generic appliance. This field will be empty if a URL is not available.
- Custom Field 1-3 - Custom fields that have been assigned to units. If these fields have been defined with new names, the defined names will appear instead of Custom Field 1, Custom Field 2 and Custom Field 3. See *Managing units by custom fields* on page 144 for more information.
- Department - Department name assigned to units. See *Grouping units by department* on page 138 for more information.
- DSView Software Server - Name of the server associated with the units.
- Location - Location assigned to the units. See *Grouping units by location* on page 140 for more information.
- Migration Status - Whether units from an imported DSView 2.x database or CCM appliances using AVWorks® software require migration to be operational in the DSView management software. See *Importing DSView 2.x software databases* on page 247 for more information.
- Model Number - Model numbers. See *Changing Unit Properties* on page 99 for more information.
- Part Number - Part numbers. See *Changing Unit Properties* on page 99 for more information.
- Primary Contact, Primary Contact Phone, Secondary Contact and Secondary Contact Phone - Name of the person who is responsible for a unit. See *Specifying user phone contact information* on page 160 for more information.
- Serial Number - Serial numbers of units. See *Changing Unit Properties* on page 99 for more information.
- Telnet Port - Port number used for a Telnet connection to a target device.
- Visibility - Whether to display (Show) or not display (Hide) a unit in the Unit Views windows.

See *Using the Customize link in windows* on page 15 for more information.

About Embedded Units

The IBM ASM RSA II and the DRAC 4 embedded units have one target port and one appliance for each embedded appliance.

The NEC IPF embedded unit has nine target ports and one appliance for each embedded appliance. Port names default to “Blade” plus the port number.

The Compaq iLO embedded unit has one target device.

In the DSView software, each of these appliance types will contain specific information about the target as well as the embedded appliance itself. All KVM connections are initiated through the target port/device.

After an embedded appliance type is added to the DSView software, an appliance type is added under the Appliances link in the side navigation bar.

Updating firmware, changing device settings and rebooting embedded units must be done manually. See the embedded units’ documentation for further information.

Launching embedded unit sessions

From the Target Devices window, users may launch a KVM or browser session to the embedded devices. Each session is handled by the embedded unit and is launched in a separate window browser. Compaq iLO, NEC IPF, IBM ASM RSA II and DRAC 4 viewers are proprietary to their owners, and the DSView software has little control of their look, feel and configuration.

There is no status polling for these sessions (status is idle by default); nor are there connection types. All embedded KVM browsers have their own certificate authentication. Users must accept certificate authentication to launch embedded unit video sessions.

Users must manually close the window to close a session. In all cases, exiting or logging out of the DSView software will not shut the KVM/browser session.

- The DRAC 4 KVM session launches a standalone launch browser which in turn launches a KVM applet. To leave the session, the user must exit the KVM session applet and the standalone launch browser.
- The IBM ASM RSA II KVM session launches a KVM session applet within a browser. To leave the session, users must exit the KVM browser session.
- The NEC IPF KVM session launches a standalone KVM session applet. To leave the session, users must exit the standalone KVM session.
- The Compaq iLO session will launch a browser session to the login page of the embedded device server. Users must log in to the web server to access the target device’s KVM session. To leave the session, users must exit the KVM browser session.

See the embedded units’ documentation for further information.

Adding Units

You may add:

- A single managed appliance
- A single embedded appliance
- Multiple managed appliances based on a range of IP addresses

- A single target device that is not attached to a managed appliance

NOTE: A DSI5100 appliance may be attached to only one DSView software system at a time.

When a managed appliance is added, DSView software administrator, user administrator and appliance administrator privileges are automatically assigned to the managed appliance. A user with any of these privileges may:

- Reboot a managed appliance and disconnect sessions
- Administer local user accounts on the managed appliance
- Control target device power
- Establish sessions with target devices from the DS1800 digital switch, CPS appliance, CCM appliance or DSR switch, or establish sessions with BMCs attached to a DSI5100 appliance as target devices.

Appliance administrators and DSView software administrators may:

- Flash upgrade a managed appliance
- View and configure settings for a managed appliance

Managed appliance rights may be changed. See *Changing Unit Access Rights* on page 102 for more information.

An SPC device is automatically added to the DSView software database and associated with the specified serial port on a DSR switch, CPS appliance or CCM appliance when you add the managed appliance. Any target devices plugged into the SPC device outlets are also added, based on the options selected.

The applicable X.509 certificate is automatically copied from the DSView management software to the DS1800 digital switch, DSI5100, CPS or CCM appliance or DSR switch being added. A certificate is a unique identifier of an individual managed appliance.

NOTE: EVR1500 environmental monitors and generic appliances do not support certificates and may be added to multiple DSView software systems.

To add a single managed appliance:

NOTE: This procedure is valid for the following managed appliances: DS1800 digital switch, DSI5100 appliance, CPS appliance, CCM appliance or DSR switch.

1. Click *Add* in a Unit Views window. The Add Unit Wizard will open. Click *Next*.
2. The Select Add Unit Procedure window will open. Click *Add a single appliance*, then click *Next*.
3. The Select Appliance Type window will open. Select a managed appliance from the product list, then click *Next*.
4. A Select Address Configuration of Appliance window will open, including the type of the managed appliance.

Click *No, the <Managed Appliance Type> does not have an address* if the managed appliance does not have an existing address. Continue to step 5.

-or-

Click *Yes, the <Managed Appliance Type> does have an address* and either type the address or the fully qualified domain name for the managed appliance. Go to step 7.

5. The Configure Appliance Network Settings window will open.
   a. Type the IP address and subnet mask, in standard dot notation (xxx.xxx.xxx.xxx), for the managed appliance.
   b. Optionally, type a gateway in standard dot notation (xxx.xxx.xxx.xxx).
   c. Click *Next*.
6. The Select Appliance to Add window will open. Select the entry, then click *Next*.
7. The Select Options window will open. (This window will not appear when adding a CCM appliance that is using firmware compatible with AVWorks software; see *Task: Migrating AVWorks software CCM appliances to DSView software compatible units* on page 265 for more information.)
   a. Click *Enable secure mode* if you want the managed appliance to only be accessible by this DSView software system. In non-secure mode, the managed appliance may be added to multiple DSView software systems.

      This checkbox will not appear when adding a DSI5100 appliance, which may only be added in Secure mode.
   b. Click *Allow target devices that contain default names to be added* if you wish to add any target devices whose port names have not been modified from the factory defaults of the managed appliance.

      This checkbox has no effect when adding a DSI5100 appliance, since default target device names are not supported. A target device is named when it is added as a BMC port using the Add IPMI BMC Wizard.
   c. Click *Allow target devices with the same name to be merged into a single target device* if you wish to merge a target device that has multiple connections into a single target device.

      For example, a target device may be connected to a both a DSR switch and an SPC device outlet connected to a CPS appliance.
   d. Click *Next*.

      If you are adding a DS1800 digital switch, CPS or CCM appliance or DSR switch, continue to step 8.

      -or-

      If you are adding a DSI5100 appliance, go to step 9.
8. If one or more cascade switches are connected to the managed appliance, the Configure Cascade Switches window will open.

a. Select the type of cascade switch for each row from the drop-down menu in the Cascade Switch Type column.

b. If you wish, type a name for each row in the Name column.

c. If two or more rows of a multiuser cascade switch are discovered, you may merge the rows by selecting the checkboxes of those rows and clicking *Merge*. To undo the merge, click the row of the merged switch and click *Split*.

d. Click *Next*.

9. The Completed Successful window will open.

   When you add a CCM appliance that is using firmware compatible with AVWorks software, you will be alerted that it must be migrated, along with a link named Add Migration Task, which will take you to the Add Task Wizard.

10. Click *Finish.*

To add a single embedded appliance:

NOTE: This procedure is valid only for IBM ASM RSA II, DRAC 4, Compaq iLO and NEC IPF embedded appliances.

1. Click *Add* in a Unit Views window. The Add Unit Wizard will open. Click *Next*.
2. The Select Add Unit Procedure window will open. Click *Add a single appliance*, then click *Next*.
3. The Select Appliance Type window will open. Select an embedded appliance from the product list, then click *Next*.

   For an IBM ASM RSA II embedded appliance, continue to step 4.

   For a DRAC 4 embedded appliance, continue to step 5.

   For a Compaq iLO embedded appliance, continue to step 6.

   For an NEC IPF embedded appliance, continue to step 7.

4. For IBM ASM RSA II embedded appliances:

   a. The Configure IBM ASM RSA II Settings window will open.

   b. In the Appliance Name field, type a 1-64 character appliance name. The name is not case sensitive.

   c. In the Address field, type a 1-256 character IP address in dot notation form or a DNS name. The address is not case sensitive.

   d. In the Username field, type a 1-64 character username to be used to log in to the embedded appliance. Usernames are case sensitive.

   e. In the Password field, type a 1-64 character password to be used to log in to the embedded appliance. Passwords are case sensitive.

   f. Click *Next*.

g. The embedded device discovery will verify that a web server exists at the specified IP address. If successful, the Select Option window will open.

h. Enable or disable the *Allow target devices with the same name to be merged into a single target device* checkbox.

i. Click *Next*. Continue to step 8.

5. For DRAC 4 embedded appliances:
   a. The Configure DELL DRAC4 Settings window will open.
   b. In the Appliance Name field, type a 1-64 character appliance name. The name is not case sensitive.
   c. In the Address field, type a 1-256 character IP address in dot notation form or a DNS name. The address is not case sensitive.
   d. In the Port field, type a TCP port number in the range 0-65535 where the appliance will listen.
   e. In the Username field, type a 1-64 character username to be used to log in to the embedded appliance. Usernames are case sensitive.
   f. In the Password field, type a 1-64 character password to be used to log in to the embedded appliance. Passwords are case sensitive.
   g. Click *Next*.
   h. The embedded device discovery will verify that a web server exists at the specified IP address. If successful, the Select Option window will open.
   i. Enable or disable the *Allow target devices with the same name to be merged into a single target device* checkbox.
   j. Click *Next*. Continue to step 8.
6. For Compaq iLO embedded appliances:
   a. The Configure COMPAQ iLO Settings window will open.
   b. In the Appliance Name field, type a 1-64 character appliance name. The name is not case sensitive.
   c. In the Address field, type a 1-256 character IP address in dot notation form or a DNS name. The address is not case sensitive.
   d. Click *Next*. Continue to step 8.
7. For NEC IPF embedded appliances:
   a. The Configure NEC IPF Settings window will open.
   b. In the Address field, type a 1-256 character IP address in dot notation form or a DNS name. The address is not case sensitive.
   c. In the Username field, type a 1-64 character username to be used to log in to the embedded appliance. Usernames are case sensitive.

d. In the Password field, type a 1-64 character password to be used to log in to the embedded appliance. Passwords are case sensitive.

e. Click *Next*.

f. The embedded device discovery will verify that the embedded appliance's product ID matches the appliance type. If successful, the Select Options window will open.

g. The Appliance Name field contains the name stored in the embedded appliance. You may change this to a 1-256 character unique name. Names are not case sensitive.

h. Enable or disable the *Allow target devices with the same name to be merged into a single target device* checkbox.

i. Click *Next*.

8. The Completed Successful window will open.
9. Click *Finish*.

To add a managed appliance from a range of IP addresses:

NOTE: This procedure is valid for the following managed appliances: DS1800 digital switch, DSI5100 appliance, CPS appliance, CCM appliance or DSR switch.

1. Click *Add* in a Unit Views window. The Add Unit Wizard will open. Click *Next*.
2. The Select Add Unit Procedure window will open. Click *Discover appliances on the network from an IP address range*, then click *Next*.
3. The Type in Discover IP Address Range window will open.
   a. Type the IP address in standard dot notation (xxx.xxx.xxx.xxx), from which to begin the search.
   b. Type the IP address in standard dot notation (xxx.xxx.xxx.xxx), at which to end the search.
   c. Click *Next*.
4. The DSView software will search for managed appliances within the IP address range. When the search is completed, the Select Appliances to Add window will open, listing the results.
5. Specify the managed appliance(s) you wish add:
   a. Select a managed appliance in the Appliances found list. Multiple managed appliances may be selected by pressing **Ctrl** while clicking on the managed appliance names.
   b. Click *Add*. The managed appliance(s) will be moved to the Appliances to Add list.

      To remove selected managed appliances, select the managed appliance you wish to remove from the Appliances to Add list (multiple managed appliances may be selected by pressing **Ctrl** while clicking on the managed appliance names) and then click *Remove*. The managed appliances will be moved to the Appliances found list.
   c. Click *Next*.
6. The Select Options window will open.

a. Click *Enable secure mode* if you want the managed appliance to only be accessible by this DSView software system. In non-secure mode, the managed appliance may be added to multiple DSView software systems.

   This checkbox will not appear when adding a DSI5100 appliance, which may only be added in Secure mode.

   This checkbox will not appear when adding a CCM appliance that is using firmware compatible with AVWorks software. The option will be displayed when the appliance is migrated to DSView software (see *Task: Migrating AVWorks software CCM appliances to DSView software compatible units* on page 265).

b. Click *Allow target devices that contain default names to be added* if you wish to add any target devices whose port names have not been modified from the factory defaults of the managed appliances.

   This checkbox has no effect when adding a DSI5100 appliance, since default target device names are not supported. A target device is named when it is added as a BMC port using the Add IPMI BMC Wizard.

c. Click *Allow target devices with the same name to be merged into a single target device* if you wish to merge a target device that has multiple connections into a single target device. For example, a target device may be connected to a both a DSR switch and an SPC device outlet connected to a CPS appliance.

d. Click *Next.*

7. The Adding Appliances window will open while the selected managed appliances are added to the DSView software system.
8. The Completed Successful window will open.

   When you add a CCM appliance that is using firmware compatible with AVWorks software, you will be alerted that it must be migrated, along with a link named Add Migration Task, which will take you to the Add Task Wizard.
9. Click *Finish.*

To add a single EVR1500 environmental monitor or generic appliance:

1. Click *Add* in a Unit Views window. The Add Unit Wizard will open. Click *Next*.
2. The Select Add Unit Procedure window will open. Click *Add a single appliance*, then click *Next*.
3. The Select Appliance Type window will open. Select *EVR1500* or *Generic* from the product list, then click *Next.*
4. A Configure Generic Appliance Settings window will open, including the name of the EVR1500 environmental monitor or generic appliance.
   a. Type the name.
   b. (Optional) Type either the address or the fully qualified domain name.
   c. (Optional) Type the Telnet port.

d. (Optional) Type the web browser URL.
e. Click *Next*.

5. The Completed Successful window will open.
6. Click *Finish*.

To add a target device:

1. Click *Add* in a Unit Views window. The Add Unit Wizard will open. Click *Next*.
2. The Select Add Unit Procedure window will open. Click *Add a single target device*. Click *Next*.
3. The Type in Device Settings window will open, where you may type the name and other optional information.
   a. Type the name.
   b. Type either the address or the fully qualified domain name.
   c. Type the Telnet port.
   d. Type the web browser URL.
   e. Click *Next*.
4. The Completed Successful window will open.
5. Click *Finish*.

Managing Units

The following items may be modified for units:

- Overview
- Credentials (supported IBM, DELL and NEC embedded units only)
- Properties
- Access Rights (displays only for users who are administrators or user administrators)
- Appliance Settings (DS1800 digital switches, CPS appliances, CCM appliances and DSR switches only)
- IPMI (DSI5100 appliances only) - see *Displaying Sensor Information by Selecting an IPMI 1.5 Target Device* on page 233 for more information
- Connections (DS1800 digital switches, DSI5100 and CPS appliances, CCM appliances, DSR switches and target devices only)

Changing Unit Overview Information

The Unit Overview window contains the following information:

- Target Devices - This window contains the name, type and icon associated with the target device. You may also use this window to connect to the target device. The available connection methods are determined by the type of target device.

  Power information appears only if the target device is connected to an SPC device outlet and the user has power control rights. In this case, the user may power up, power down or cycle the power of the target device.
- Target Devices with a DSI5100 IPMI connection - This window contains the name, type and icon associated with the IPMI 1.5 target device, the power state of the target device chassis power and tools that may be used to:
  - Start an IPMI session with the IPMI 1.5 target device.
  - Perform a hard reset of the IPMI 1.5 target device.
  - Turn the identity light emitting diode (LED) on the IPMI 1.5 target device on or off. If the BMC does not have a fixed interval, the LED will turn on or off for 45 seconds.
  - Power up, power down, cycle the power or perform a graceful shutdown of the IPMI 1.5 target device.

  Other icons may appear, based on connections to other units.
- Managed appliances - This window contains the name and type of managed appliances and the tools that may be used to:
  - Reboot
  - Upgrade firmware
  - Resynchronize
  - Save or restore the configuration (valid only for DS1800 digital switches, CPS and CCM appliances and DSR switches)
  - Save or restore the user database (valid only for CPS and CCM appliances and certain DSR switches)

  The available tasks depend on the type of managed appliance and the user's rights on the managed appliance.
- EVR1500 environmental monitor or generic appliance - This window contains the name and type of EVR1500 environmental monitor or generic appliance and links for establishing a connection to it.

NOTE: The Type field of managed appliances cannot be modified.

To change target device overview information:

1. Click *Units* in the tab bar. *Unit Views - Target Devices - All* will automatically be selected in the side navigation bar.
2. Click on the name of a target device. The Unit Overview window will open.
3. Type a name for the target device.
4. Type a new type for the target device.

5. Select a new icon for the target device using the arrows.
6. Click *Save* and then click *Close*. The Unit Views window will open, including the new information for the target device. If you added a type that was not previously defined, it will appear under Target Devices in the side navigation bar.

To start a session with a target device from the Unit Overview window:

1. Click *Units* in the tab bar. *Unit Views - Target Devices - All* will automatically be selected in the side navigation bar.
2. Click on the name of a target device. The Unit Overview window will open.
3. Click on the icon or name of the session type you wish to start.

To change the power state of a target device:

NOTE: A user must have power control privileges and the target device must be connected to and powered by an SPC device outlet.

1. Click *Units* in the tab bar. *Unit Views - Target Devices - All* will automatically be selected in the side navigation bar.
2. Click on the name of a target device. The Unit Overview window will open.
3. Click the checkbox to the left of the SPC device outlet for which you wish to change the power state.

   -or-

   Click the checkbox to the left of Connection at the top of the list to select all SPC device outlets listed in the window.
4. Click *On* to power up the SPC device outlets.

   -or-

   Click *Off* to power down the SPC device outlets.

   -or-

   Click *Cycle* to cycle the power (power down and then power up) on the target device connected to the SPC device outlet.

To change the name of a managed appliance:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar and then click on the type of appliance.
3. Click on the name of an appliance. The Unit Overview window will open.
4. Type a name for the managed appliance.
5. Click *Save* and then click *Close*. The Unit Views window will open, including the new name of the managed appliance.

Changing Embedded Unit Credentials

You may change the login credentials for the IBM ASM RSA II, DRAC 4 and NEC IPF embedded units.

To change login credentials for an IBM ASM RSA II embedded appliance:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar, and then click on the appliance type in the side navigation bar.
3. Click on the embedded appliance name.
4. Click the *Credentials* link in the side navigation bar and then click *Credentials* in the side navigation bar.
5. The IBM ASM RSA II Settings window will open.
6. In the Appliance Name field, type a 1-64 character appliance name. The name is not case sensitive.
7. In the Username field, type a 1-64 character username to be used to log in to the embedded appliance. Usernames are case sensitive.
8. In the Password field, type a 1-64 character password to be used to log in to the embedded appliance. Passwords are case sensitive.
9. Click *Save* and then click *Close*.

To change login credentials for a DRAC 4 embedded appliance:

1. Click *Units* in the tab bar. *Units* will automatically be selected in the top navigation bar.
2. Click *Appliances* in the side navigation bar and then click on the appliance type in the side navigation bar.
3. Click the embedded appliance name.
4. Click the *Credentials* link in the side navigation bar and then click *Credentials* in the side navigation bar.
5. The DELL DRAC4 Settings window will open.
6. In the Appliance Name field, type a 1-64 character appliance name. The name is not case sensitive.
7. In the Port field, type a TCP port number in the range 0-65535 where the appliance will listen.
8. In the Username field, type a 1-64 character username to be used to log in to the embedded appliance. Usernames are case sensitive.
9. In the Password field, type a 1-64 character password to be used to log in to the embedded appliance. Passwords are case sensitive.
10. Click *Save* and then click *Close*.

To change login credentials for an NEC IPF embedded appliance:

1. Click *Units* in the tab bar. *Units* will automatically be selected in the top navigation bar.
2. Click *Appliances* in the side navigation bar.
3. Click the embedded appliance name.
4. Click the *Credentials* link in the side navigation bar and then click *Credentials* in the side navigation bar.
5. The NEC IPF Settings window will open.
6. In the Name field, type a 1-64 character appliance name. The name is not case sensitive.
7. In the Username field, type a 1-64 character username to be used to log in to the embedded appliance. Usernames are case sensitive.
8. In the Password field, type a 1-64 character password to be used to log in to the embedded appliance. Passwords are case sensitive.
9. Click *Save* and then click *Close*.

Changing Unit Properties

A user with access rights may change the following properties for a unit:

- Identity - May be helpful for quickly identifying information about a unit.
- Location - May be helpful for identifying where a unit is. If no sites, departments or locations are available, they may be added. See *Grouping units by site* on page 135, *Grouping units by department* on page 138 and *Grouping units by location* on page 140 for more information.
- Contacts - Identify the primary and secondary contacts for a unit that will appear in the Unit Views window. Assigning contact properties may be helpful for quickly identifying the people to notify if an issue or question arises about a particular unit.
- Custom Fields - Three custom fields are available, in which you may specify any information you wish. For example, you may wish to define custom fields such as Program Manager, Building Number and so on. See *Managing units by custom fields* on page 144 for more information.
- Notes
- Network

Some properties display by default in a Unit Views window. Others must be displayed by using the *Customize* link. See *Using the Customize link in windows* on page 15 for more information.

To change the unit identity properties:

NOTE: Identity properties are visual representations only. Defining incorrect information may cause confusion (for example, mistyping a serial number).

1. Click *Units* in the tab bar.
2. Click *Appliances* or *Target Devices* in the side navigation bar.

3. Click a unit type in the side navigation bar, if configured.
4. Click on the appliance or target device name.
5. Click *Properties* in the side navigation bar. *Identity* will automatically be selected and the Unit Identification Properties window will open.
6. Type a part number, serial number, model number and/or asset tag number.
7. Click *Save* and then click *Close*. The Unit Views window will open, including any changes.

To change the unit location properties:

NOTE: Location properties are visual representations only. Defining incorrect information may cause confusion (for example, a mistyped room number).

1. Click *Units* in the tab bar.
2. Click *Appliances* or *Target Devices* in the side navigation bar.
3. Click a unit type in the side navigation bar, if configured.
4. Click on the appliance or target device name.
5. Click *Properties* in the side navigation bar and then click *Location* in the side navigation bar. The Unit Location Properties window will appear.
6. Type or use the drop-down lists to select the site, department and/or location where the unit is located.
7. Click *Save* and then click *Close*. The Unit Views window will open, including any changes.

To change the contact properties of a unit:

NOTE: Contact properties should be kept up-to-date.

1. Click *Units* in the tab bar.
2. Click *Appliances* or *Target Devices* in the side navigation bar.
3. Click a unit type in the side navigation bar, if configured.
4. Click on the appliance or target device name.
5. Click *Properties* in the side navigation bar and then click *Contacts* in the side navigation bar. The Unit Contacts window will open.
6. Type the names and phone numbers of the primary and secondary contacts.
7. Click *Save* and then click *Close*. The Unit Views window will open, including any changes.

To change the custom fields of a unit:

1. Click *Units* in the tab bar.
2. Click *Appliances* or *Target Devices* in the side navigation bar.
3. Click a unit type in the side navigation bar, if configured.
4. Click on the appliance or target device name.

5. Click *Properties* in the side navigation bar, then click *Custom Fields* in the side navigation bar. The Unit Custom Fields window will open.
6. Type the information in each of the three custom fields.
7. Click *Save* and then click *Close*. The Unit Views window will open, including any changes.

To change the note properties of a unit:

1. Click *Units* in the tab bar.
2. Click *Appliances* or *Target Devices* in the side navigation bar.
3. Click a unit type in the side navigation bar, if configured.
4. Click on the appliance or target device name.
5. Click *Properties* in the side navigation bar and then click *Notes* in the side navigation bar. The Unit Notes window will open.
6. Type description, accounting and comment information.
7. Click *Save* and then click *Close*. The Unit Views window will open, including any changes.

To change the network properties of a target device:

NOTE: Defining incorrect information for these properties may cause network connection errors.

1. Click *Units* in the tab bar. *Unit Views - Target Devices - All* will automatically be displayed in the side navigation bar.
2. Click on the target device name.
3. Click *Properties* in the side navigation bar and then click *Network* in the side navigation bar. The Unit Network Properties window will open.
4. Type the address or the fully qualified domain name for the target device.
5. Type the Telnet port number to use for Telnet connections to the target device. If this field is left blank, Telnet will not be enabled for the target device.
6. Type the URL for a web browser connection to the target device.
7. Select the DSView software server that is in charge of the target device.
8. Click *Save* and then click *Close*. The Unit Views window will open, including any changes.

To change the network properties of a managed appliance:

NOTE: This procedure is valid for the following managed appliances: DS1800 switches, DSI5100 appliances, CPS appliances, CCM appliances and DSR switches.

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar.
3. Click an appliance type in the side navigation bar, if configured.
4. Click on the appliance name.

5. Click *Properties* in the side navigation bar and then click *Network* in the side navigation bar. The Unit Network Properties window will open.
6. Type the address or the fully qualified domain name.

   If you are changing the appliance IP address, you should first change it in the Appliance Network Settings window before changing it in the Unit Network Properties window. See *Changing Managed Appliance Settings* on page 106 for more information.
7. Select the DSView software server in charge of the managed appliance.
8. Click *Save* and then click *Close*. The Unit Views window will open, including any changes.

To change the network properties of an EVR1500 environmental monitor or generic appliance:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar.
3. Click an appliance type in the side navigation bar, if configured.
4. Click on the appliance name.
5. Click *Properties* in the side navigation bar and then click *Network* in the side navigation bar. The Unit Network Properties window will open.
6. Type the address or the fully qualified domain name.
7. Type a Telnet port number.
8. Type a web browser address.
9. Select the DSView software server in charge of the EVR1500 environmental monitor or generic appliance.
10. Click *Save* and then click *Close*. The Unit Views window will open, including any changes.

Changing Unit Access Rights

Access rights indicate which users and user groups may access a unit.

Access rights also indicate which actions are allowed.

For target devices, you may specify whether a user or members of a user group are allowed to:

- Establish a serial session on target devices
- Establish a Video Viewer session on target devices
- Power up, power down or cycle the power of target devices
- Establish virtual media sessions to target devices
- Establish reserved virtual media sessions to target devices

For certain managed appliances (DS1800 digital switch, DSI5100, CPS and CCM appliances and DSR switches), you may specify whether a user or members of a user group are allowed to:

- Reboot the managed appliance and/or disconnect sessions
- Upgrade the firmware (Flash)

- Configure managed appliance settings
- Configure local user accounts (valid only on CPS and CCM appliances and supported DSR switches)

For example, you may allow users to configure settings on a managed appliance, but not allow them to reboot and disconnect sessions on it. Instead, you may allow a user who has appliance administrator privileges on the target devices to establish a Video Viewer session, but not allow that user to perform power control operations. Access rights may also be specified for all units in the DSView software system or for a specific unit.

By default, supported embedded units have the same access rights as generic units. The DSView software administrator may change the user/group access and access rights.

To add or remove user/user group managed appliance access and access rights:

NOTE: Except as noted, this procedure is valid on the following managed appliances: DS1800 digital switches, DSI5100 appliances, CPS appliances, CCM appliances, DSR switches and supported embedded units.

1. Click *Units* in the tab bar. From a Unit Views window:

   To add/remove access to a single managed appliance, click on a managed appliance name. *Overview* will automatically be selected in the side navigation bar and the Unit Overview window will open. Continue to step 2.

   -or-

   To add/remove access to all managed appliances, do not select any checkboxes and click the *Rights* button. Go to step 3.

   -or-

   To add/remove access to selected appliances, click the checkboxes next to the units, and then click the *Rights* button. Go to step 3.

2. From the side navigation bar, click *Access Rights*. The Unit Access Rights window will open.
3. To add or remove a user or user group from the Access Rights Assignment list, click *Edit List*. The Unit Access Rights User Selection window will open.

   To add a user or user group:

   a. Select the user or user group you wish to add in the Available list. Multiple users and/or user groups may be selected by pressing **Ctrl** while clicking on the names.

   b. Click *Add*. The users and user groups will be moved to the List to Update list.

   To remove a user or user group:

   a. Select the user or user group you wish to remove from the List to Update list. Multiple columns may be selected by pressing **Ctrl** while clicking on the names.

   b. Click *Remove*. The users and user groups will be moved to the Available list.

   Click *OK*. The Assign Access Rights window will display the current list of users and/or user groups. When a user or user group is added to the list, default access rights will be displayed in the Unit Access Rights window.

4. To add/remove access rights for a user/user group, select a user or group in the User and User Groups list, then enable or disable the *Allow* checkbox next to the access right. Select one or more of the following:
   a. *Reboot Appliance and Disconnect Sessions* - enables the user or members of the group to reboot the appliance and disconnect active sessions.
   b. *Flash Upgrade Appliance* - enables the user or members of the group to upgrade the firmware (Flash) on the appliance.
   c. *Configure Unit Settings* - enables the user or members of the group to configure appliance settings.
   d. *Configure Appliance Local User Accounts* - enables the user or members of the group to configure local user accounts on CPS or CCM appliances and supported DSR switches.

      The Local User Accounts options is not valid on other managed appliances and will not appear in the Unit Access Rights window.
5. Repeat step 4 to change access rights for other users or user groups.
6. Click *Save* and then click *Close*. The Unit Views window will open.

About target device access rights

When you assign access rights to a target device, any available session types may be selected, even if the target device does not support them. For example, you may enable Video Viewer and virtual media sessions to a target device that is attached to a CCM appliance, which does not support virtual media.. The target device access rights are not based on the valid type of connection to that target device - the ability to establish a particular session type exists only when the target device (through its managed appliance) supports it. Using the above example, if the target device that was attached to the CCM appliance was later moved to a managed appliance that supported virtual media sessions, the target device could then be accessed by that method.

Each access right is independent of other access rights. For example, you may enable virtual media session access to a target device that supports it, but not enable KVM (Video Viewer) session access to that target device. Since a virtual media session is launched from a KVM session, that user would, in fact, not be able to open a virtual media session with that target device. The access right only indicates that the user is allowed to perform the operation; it does not mean that the operation can actually be performed.

To add or remove user/user group target device access and access rights::

NOTE: Only users in the DSView software administrator, appliance administrator and user administrator user groups may configure unit access rights.

1. Click *Units* in the tab bar. From a Unit Views window:

   To change the access rights for a single target device, click on a target device name. *Overview* will automatically be selected in the side navigation bar and the Unit Overview window will open. Continue to step 2.

   -or-

To change the access rights of all devices, click the *Rights* button. The Unit Access Rights window will open. Go to step 4.

-or-

To change the access rights of a selected target device, click the checkboxes next to the target device names and then click the *Rights* button. Go to step 3.

2. From the side navigation bar, click *Access Rights*. The Unit Access Rights window will open.
3. To add or remove a user or user group from the list, click *Edit List*. The Unit Access Rights User Selection window will open.

   To add a user or user group:

   a. Select the user or user group you wish to add in the Available list. Multiple users and/or user groups may be selected by pressing **Ctrl** while clicking on the names.

   b. Click *Add*. The users and user groups will be moved to the List to Update list.

   To remove a user or user group:

   a. Select the user or user group you wish to remove from the List to Update list. Multiple columns may be selected by pressing **Ctrl** while clicking on the names.

   b. Click *Remove*. The users and user groups will be moved to the Available list.

   Click *OK*. The Assign Access Rights window will display the current list of users and/or user groups. When a user or user group is added to the list, default access rights will be displayed in the Unit Access Rights window.
4. To add/remove access rights for a user/user group, select a user or group in the User and User Groups list, then enable or disable the *Allow* checkbox next to the access right. Select one or more of the following.

   a. *Configure Unit Settings* - enables the user or members of the user group to configure settings for this target device.

   b. *Establish Viewer Sessions* - enables the user or members of the user group to establish a Video Viewer session with the target device.

   c. *Establish Virtual Media Sessions* - enables the user or members of the user group to establish a virtual media session with the target device. Since virtual media sessions are launched from a Video Viewer session, if you select this option, you should also select *Establish Viewer Sessions.*

   d. *Establish Reserved Virtual Media Sessions* - enables the user or members of the user group to establish a Reserved Virtual Media session with the target device. Since virtual media sessions are launched from a Video Viewer session, if you select this option, you should also select *Establish Viewer Sessions.*

   e. *Control Target Device Power* - enables the user or members of the user group to power up, power down or cycle power to the target device.
5. Repeat steps 3 and 4 to change access rights for other users or user groups.

6. Click *Save* and then click *Close*. The Unit Views window will open. If enabled, a KVM Session, Virtual Media Session or Serial Session link will appear in the Action column. If enabled, a power control option will appear in the Unit Overview window.

Changing Managed Appliance Settings

You may display and change the following settings for a DS1800 digital switch, CPS appliance, CCM appliance or DSR switch:

- Network settings
- Authentication server
- NFS settings and status (CCM appliances only)
- NTP settings and status for (CCM appliances only)
- SNMP settings, including enabling/disabling SNMP, the IP addresses of service managers and destinations and community names
- Version numbers of software and firmware
- Port management, including upgrading of DSRIQ modules, cascade switches, SPC devices and mode OSCAR interface authentication
- Session management, including changing settings, viewing and disconnecting sessions and specifying global macros
- Adding, removing and changing the local CPS or CCM appliance or DSR switch account

The following appliance settings may be modified for a DSI5100 appliance:

- Version number of the hardware and firmware
- Appliance port management, including adding and deleting BMCs

NOTE: The MAC address may not be modified.

To change the network settings of a managed appliance:

NOTE: Except as noted, this procedure is valid on the following managed appliances: DS1800 digital switches, CPS appliances, CCM appliances and DSR switches.

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *Network*. The Appliance Network Settings window will open.
5. Type an IP address, in standard dot notation (xxx.xxx.xxx.xxx). If you change the IP address of an appliance in the Appliance Network Settings window, you must then also change the address in the Unit Network Properties window. See *Changing Unit Properties* on page 99 for

more information. (When changing an IP address, always change it in the Appliance Network Settings window before changing it in the Unit Network Properties window.)

6. Type a subnet, in standard dot notation (xxx.xxx.xxx.xxx).
7. Type a gateway, in standard dot notation (xxx.xxx.xxx.xxx)
8. Use the drop-down menu to specify a LAN speed. This network setting will not appear for CPS appliances.
9. Use the drop-down menu to enable or disable DHCP or BootP (DS1800 digital switches and DSR switches).
10. Use the drop-down menu to enable or disable ICMP ping reply.
11. Click *Save* and then click *Close*. The Unit Views window will open.

To change the IP addresses of authentication servers:

NOTE: Except as noted, this procedure is valid for the following managed appliances: DS1800 digital switches, CPS appliances, CCM appliances and DSR switches.

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *Authentication Servers*. The Appliance Authentication Servers Settings window will open.
5. Type an IP address, in standard dot notation (xxx.xxx.xxx.xxx), for up to four authentication servers.
6. Click *Save* and then click *Close*. The Unit Views window will open.

To display NFS status or change the NFS settings for a CCM appliance:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *NFS*. The Appliance NFS Settings window will open.
5. To enable NFS on the appliance, click the *Enable NFS* checkbox. To disable NFS, uncheck it.

   When you enable NFS, you may also configure the following information:

   a. Type an address in the *NFS Server* field.
   b. Type the mount point in the *NFS Mount Point* field.
   c. Select the protocol to be used from the *Protocol* drop-down menu.

d. Choose the log file rotation type by enabling one of the radio buttons *Do not rotate*. *Append data to end of file* or *Create new file each day at midnight*.

6. Click *Save* and then click *Close*. The Unit Views window will open.

The NFS Status section of the Appliance NFS Settings window may contain one of the values described in Table 4.3.

Table 4.3: CCM Appliance NFS Status Values

Status	Description
Not mounted	NFS is not currently enabled.
Mounted	NFS is currently enabled and is currently successfully mounted.
Mounting	NFS is currently enabled and the mount is being attempted for the first time. The mount has not yet succeeded or failed.
Mount attempt failed (retrying)	NFS is currently enabled, but a mount failure has occurred and the mount is currently being retried.
Mount attempt failed (no longer retrying)	NFS is currently enabled, but a mount failure has occurred and the CCM appliance was not able to establish the mount after performing the maximum number of retries allowed. The CCM appliance has stopped trying to establish this mount.
Mount lost (retrying)	NFS is currently enabled and was successfully mounted, but a mount failure subsequently occurred. The mount is currently being retried. *
Mount lost (no longer retrying)	NFS is currently enabled and was successfully mounted, but a mount failure subsequently occurred. The CCM appliance was not able to reestablish the mount after performing the maximum number of mount retries allowed. *
Verifying existing mount	NFS is currently enabled and was successfully mounted. Another NFS Enable command was entered without changing any parameters, which triggered a mount verification, which is still in progress.

* An error message accompanying the status identifies the reason for the mount failure. See the CCM Installer/User Guide for more information.

To display NTP status or change the NTP settings for a CCM appliance:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *NTP*. The Appliance NTP Settings window will open.
5. To enable NTP on the appliance, click the *Enable NTP* checkbox. To disable NTP, uncheck it.

   When you enable NTP, you may also configure the following information:

a. Type an address in the *Primary NTP Server Address* and optionally, the *Secondary NTP Server Address* field. The primary address is required if NTP is being enabled for the first time.

b. Select or type the frequency for time updating in the *Update Interval (hours)* field. The valid range is 0-99 hours. A zero value indicates that the time should be requested and the clock updated when the CCM appliance reboots.

The NTP Status section will indicate that an update was attempted, not attempted, or is in progress.

6. Click *Save* and then click *Close*.

Changing managed appliance SNMP settings

NOTE: This procedure is valid for the following managed appliances: DS1800 digital switches, CPS appliances, CCM appliances and DSR switches.

The SNMP protocol is used to communicate management information between network management applications and DSView software managed appliances using TCP/IP and IPX protocols. Other external SNMP managers (such as Tivoli® and HP OpenView) may communicate with your managed appliances by accessing MIB-II (Management Information Base) and the public portion of the enterprise MIB. MIB-II is a standard MIB that many SNMP target devices support. The managed appliances will send their traps directly to the external SNMP manager in addition to sending it to the server.

The following settings appear beneath SNMP in the side navigation bar:

- System - Enables/disables SNMP
- Managers - Stations that may manage the managed appliance
- Community - Communities to which the traps belong
- Destinations - Stations that may receive SNMP traps
- Traps - Available traps and enabled/disabled traps

When you enable SNMP, the managed appliance will log SNMP received messages over UDP (User Datagram Protocol) port 161. UDP port 162 is used to listen for incoming traps.

The traps must be configured on each managed appliance using the Command Line Interface (CLI). The address of the server running the DSView management software must be configured as a trap recipient, the proper community must be set and each desired trap must be enabled.

All SNMP traps are logged in the event log file. See *Event Logs* on page 275 for more information.

To enable or disable SNMP system settings for a managed appliance:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.

4. Click *Appliance Settings* in the side navigation bar and then click *SNMP. System* will automatically be selected in the side navigation bar and the Appliance SNMP System Settings window will open.
5. Select *Enabled* in the Enable SNMP drop-down menu to enable logging of SNMP traps.
6. Change the name and description of the managed appliance and type a contact.
7. Click *Save* and then click *Close*. The Unit Views window will open.

To enable or disable SNMP manager settings for a managed appliance:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *SNMP* and then *Managers*. The Appliance SNMP Manager Settings window will open.
5. Type the IP addresses, in standard dot notation (xxx.xxx.xxx.xxx), for up to four SNMP managers.
6. Click *Save* and then click *Close*. The Unit Views window will open.

To specify SNMP community settings for a managed appliance:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *SNMP* and then *Community.* The Appliance SNMP Community Settings window will open.
5. Type the SNMP community names for reading, writing and SNMP traps.
6. Click *Save* and then click *Close*. The Unit Views window will open.

To specify SNMP destination settings for a managed appliance:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *SNMP* and then *Destinations*. The Appliance SNMP Destination Settings window will open.
5. Type the IP addresses, in standard dot notation (xxx.xxx.xxx.xxx), for up to four SNMP destinations.
6. Click *Save* and then click *Close*. The Unit Views window will open.

To enable or disable SNMP traps for a managed appliance:

NOTE: SNMP traps may also be configured from a system task. See *Managing Tasks* on page 255 for more information.

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *SNMP* and then *Traps*. The Appliance SNMP Trap Settings window will open.
5. Select one of the following from the drop-down menu:

   Enabled to turn a trap on or *Disabled* to turn a trap off.

   -or-

   Enable All to turn all traps on or *Disable All* to turn all traps off.
6. Click *Save* and then click *Close*. The Unit Views window will open.

To display version information for a managed appliance:

NOTE: This procedure is valid for the following managed appliances: DS1800 digital switches, DSI5100 appliances, CPS appliances, CCM appliances and DSR switches.

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then *Versions*. The Appliance Version Information window will open, containing the following information:
   - For DS1800 digital switches and DSR switches - application, boot and Video FPGA
   - For DSR switches (except the DSR4160 switch) - may include application, boot, Video FPGA, matrix FPGA, UART FPGA, digital/application, digital/digitizer, digital/FPGA and OSCAR FPGA
   - For DSI5100 appliances - DSI5100 application and boot versions
   - For CPS and CCM appliances - bootstrap and application versions
5. Click *Close*. The Unit Views window will open.

Managing and changing port settings

To display DSRIQ module information:

1. Click *Units* in the tab bar.

2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *Ports*. *IQ Modules* will automatically be selected in the side navigation bar and the Appliance IQ Modules window will open. This window lists all modules with their EID, status, port number, application version, hardware version and interface type.
5. To display an individual module's settings, click on an IQ module. The Appliance IQ Module Settings window will open.

To delete offline DSRIQ modules:

NOTE: Any offline module will appear with a red circle and an "X" to the left of its EID. An online module will appear with a green circle to the left of its EID.

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *Ports*. *IQ Modules* will automatically be selected in the side navigation bar and the Appliance IQ Modules window will open.
5. Click *Delete Offline*. A confirmation dialog box will appear.
6. Click *Yes* to confirm or *No* to cancel.

To upgrade DSRIQ modules:

NOTE: Offline DSRIQ modules may not be selected for upgrading.

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the DSR switch name.
4. Click *Appliance Settings* in the side navigation bar and then click *Ports*. *IQ Modules* will automatically be selected in the side navigation bar and the Appliance IQ Modules window will open.
5. Click the checkbox to the left of the DSRIQ modules you wish to upgrade.

   -or-

   Click the checkbox to the left of the EID column at the top of the list to select all DSRIQ modules listed in the window for upgrading.
6. Click *Upgrade*. A confirmation dialog box will appear.

7. Click *OK* to confirm or *Cancel* to cancel.

   If the upgrade is confirmed, a yellow LED icon will appear to the left of the upgrading modules. You may click on the name of a DSRIQ module in the EID column to display its upgrade status in the Appliance Settings - Ports - IQ Modules - Settings window. When the upgrade is completed, a green circle will appear next to the modules and they may once again be selected.

   -or-

   Click *Cancel* to cancel.

To display cascade switch port settings:

NOTE: This procedure is valid for the following managed appliances: DS1800 digital switches and DSR switches.

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *Ports* and then *Cascade Switches*. The Appliance Cascade Switches window will open.
5. Click *Close* when you are finished. The Unit Views window will open.

To change local OSCAR interface authentication settings:

NOTE: This procedure is valid for the following managed appliances: all DSR switches except the DSR800, 1161, 2161 and 4160 switches.

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the DSR switch name.
4. Click *Appliance Settings* in the side navigation bar and then click *Ports* and then click *OSCAR*. The Appliance OSCAR Settings window will open.
5. Click *Disable OSCAR Authentication* to prevent the supported DSR switch from performing internal or external authentication.

   If the Disable OSCAR Authentication checkbox is not selected, the supported DSR switch will attempt external authentication using the list of authentication servers that reside in the switch. If the authentication fails, the supported DSR switch will use its internal user tables.

   If you selected *Disable OSCAR Authentication*, continue to step 6.

   -or-

   If you did not select *Disable OSCAR Authentication*, go to step 7.
6. From the drop-down menu, specify a preemption level for the DSR switch (1-4).

7. Click *Save* and then click *Close*. The Unit Views window will open.

To change modem port settings:

NOTE: This procedure is valid for the following managed appliances: DSR1020, 1021, 1022, 1024, 1030, 2020, 2030, 2035, 4020, 4030, 8020, 8030 and 8035 switches.

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *Ports* and then click *Modems*. The Appliance Modem Settings window will open.
5. Select *Modem sessions can preempt digital sessions* to enable a modem session to disconnect an existing Ethernet connection to the DSR switch.
6. Type an authentication time-out for the modem in the range of 30-300 seconds.
7. Type an inactivity time-out for the modem connection in the range of 1-60 minutes.
8. Click *Save* and then click *Close*. The Unit Views window will open.

Managing SPC device port settings

NOTE: This procedure is valid for the following managed appliances: CPS appliances, CCM appliances, DSR1021, 1022, 1024, 1031, 2020, 2035, 4020, 8020 and 8035 switches.

When using an SPC device with a CPS or CCM appliance, you must configure the CPS or CCM appliance serial port with the Target Device type SPC.

Customizing the SPC Devices Attached to Appliance window

By default, the following fields display in the Devices Attached to Appliance window. Use the *Customize* link to remove these fields.

- Description - SPC device model, such as SPC800.
- Version - SPC device version, such as Avocent SPC Version 1.0k.
- Total Load - Total amps currently used by the SPC device.

You may also display the following fields which are not displayed by default.

- Poll rate - How often a supported managed appliance polls an SPC device.
- Ports Installed - Total number of outlets on the SPC device.
- Total Load Max - Maximum amperage load for the entire SPC device.
- Total Load Min - Minimum amperage load for the entire SPC device.

See *Using the Customize link in windows* on page 15 for more information.

Customizing the SPC Sockets window

By default, the following fields display in the SPC Sockets window and may be removed using the *Customize* link:

- Power - Whether an SPC device outlet is powered up or powered down.
- Control - Status of the relay (which controls the physical power to the outlet) in comparison to the controller (which controls the relay). The relay and controller are typically in sync. If either the relay or the controller fails, one of the following will appear: On, Off, Pend On, Pend Off, Reboot or Pend Reboot.
- Module - Current status of the SPC device outlet in relation to the status in the DSView management software as follows:
  - Normal - The state of the SPC device outlet matches the state detected in the software.
  - On Fail - The software detects that the SPC device outlet is powered down, but is powered up.
  - Off Fail - The software detects that the SPC device outlet is powered up, but the SPC device outlet is powered down.
  - No Response - The software is not receiving a response from the SPC device outlet.
- Minimum On (Seconds) - Minimum amount of time that the SPC device outlet will be powered up.
- Minimum Off (Seconds) - Minimum amount of time that the SPC device outlet will be powered down.

Wake - Wake-up state of the SPC device outlet, which is the state (on or off) that the port will go into when the SPC device is powered up during normal operation or when power is restored after an outage. When power is first supplied to the SPC device, all outlets are initially off. The ports are then sequenced on in two-second increments. Outlets set to a wake-up state of Off will remain off. Outlets set to a wake-up state of On will be turned on.

See *Using the Customize link in windows* on page 15 for more information.

To display or change SPC device settings:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *Ports* and then click *SPC*. The SPC Devices Attached to Appliance window will open. (For DSR switches that have two SPC device ports, one row will appear for each SPC device.)
5. Click on the name of an SPC device. *Settings* will automatically be selected in the side navigation bar and the SPC Settings window will open. The name of the SPC device will also appear under the managed appliance name in the side navigation bar.
6. Type a new description for the SPC device.

7. Type a new total minimum amp load for the SPC or use the arrow buttons to specify a new value.
8. Type a new total maximum amp load for the SPC or use the arrow buttons to specify a new value.
9. Type a polling rate in milliseconds, or use the arrow buttons to specify a new value.
10. Click *Save* and then click *Close*. The SPC Devices Attached to Appliances window will open.
11. Click *Close*. The Unit Views window will open.

To display or customize SPC device outlet settings:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *Ports* and then click *SPC*. The SPC Devices Attached to Appliance window will open.
5. Click on the name of an SPC device. *Settings* will automatically be selected in the side navigation bar and the SPC Settings window will open. The name of the outlet and SPC device will also appear under the supported managed appliance name in the side navigation bar.
6. Click *Sockets* in the side navigation bar. The SPC Sockets window will open.

   If you change the IP address of a managed appliance that is attached (in this case) to an SPC device, the managed appliance may need rebooting. In this case, a Reboot Required icon will be displayed in the top left corner of the SPC Sockets window. Click the icon to reboot the managed appliance.
7. Click on an SPC socket. The SPC Socket Settings window will open and the name of the socket will appear under the SPC device in the side navigation bar.
8. Type a new name for the socket.
9. From the drop-down menu, specify the minimum amount of time that the SPC socket should be powered up.
10. From the drop-down menu, specify a minimum amount of time that the SPC socket should be powered down.
11. From the drop-down menu, specify whether you wish to enable wake-up for the SPC device outlet.
12. Click *Save* and then click *Close*. The SPC Sockets window will open.
13. Click *Close*. The SPC Devices Attached to Appliance window will open.
14. Click *Close*. The Unit Views window will open.

To power up, power down or cycle the power of an SPC device outlet:

1. Click *Units* in the tab bar.

2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *Ports* and then click *SPC*. The SPC Devices Attached to Appliance window will open.
5. Click on the name of an SPC device. *Settings* will automatically be selected in the side navigation bar and the SPC Settings window will open. The name of the outlet and the SPC device will also appear under the managed appliance name in the side navigation bar.
6. Click *Sockets*. The SPC Sockets window will open.
7. To select a single SPC device outlet, click the checkbox to the left of the device outlet.

   -or-

   To select all SPC device outlets, click the checkbox to the left of Socket at the top of the list.
8. Click *On* to power up the selected SPC device outlets. The Power column will display On.

   -or-

   Click *Off* to power down the selected SPC device outlets. The Power column will display Off.

   -or-

   Click *Cycle* to cycle the power (power down and then power up) of the selected SPC device outlets. The Power columns will display Off and On and the Control columns will display Cycling while power is cycling. When power cycling is completed, the Power and Cycling columns will display On.

Customizing the Appliance Serial Ports window

By default, the following fields display in the Appliance Serial Ports window and may be removed using the *Customize* link:

- Port - Displays the serial port number
- Name - Displays the name of the serial port
- Type - Displays the type of port (CLI, SPC or Standard)
- Baud - Displays the baud rate of the serial port
- Data Bit - Describes the data bit rate of the serial port

See *Using the Customize link in windows* on page 15 for more information.

To display or change the general properties for a CPS or CCM appliance serial port:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.

4. Click *Appliance Settings* in the side navigation bar and then click *Ports* and then click *Serial*. The Appliance Serial Ports window will open.
5. Click on the name of a serial port. The Appliance Serial Port General Settings window will open and the name of the port will appear under the appliance in the side navigation bar.
6. Type a new name for the serial port.
7. Using the drop-down menu, specify the type of port:
   - (CPS appliances only) Standard Command Line Interface (CLI) - Select this port type if you wish to define the port as a serial connection for a local terminal.

     Only one port may be defined as a CLI port. If a second port is defined as a CLI port, the previously defined CLI port will be changed to a Standard port.
   - SPC - Select this port type if you wish to connect an SPC device to the port.
   - Standard - Select this port type if you wish to access a serial device using SSH.
8. Using the arrow buttons, specify a time-out.
9. Using the drop-down menu, specify a CLI access character that will be used to access CLI mode on a serial device. The (^) character represents the **Ctrl** key. For example, specifying ^D means that pressing **Ctrl+D** will enter CLI mode.
10. Type a Telnet port that will be used to access the serial port. The default Telnet port is 3001.
11. Using the drop-down menu, specify whether or not the port should use a DTR signal. If set to DTR, the appliance will report target devices as ON if the signal given matches the state given. Otherwise, the appliance will report the target device power as OFF.
12. Using the drop-down menu, specify a power signal type that will be used for power status monitoring of the appliance port.
13. Click *Save* and then click *Close*. The Appliances Serial Ports window will open.
14. Click *Close*. The Unit Views window will open.

To change the communication properties for a CPS or CCM appliance serial port:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *Ports* and then click *Serial*. The Appliance Serial Ports window will open.
5. Click on the name of a serial port. The Appliance Serial Ports General Settings window will open and the name of the port will appear under the appliance in the side navigation bar.
6. From the side navigation bar, click *Communication*. The Appliance Serial Port Communications Settings window will open.
7. From the drop-down menu, select a baud rate.
8. From the drop-down menu, select the number of data bits per character.

9. From the drop-down menu, select a parity rate for the serial port.
10. From the drop-down menu, select a the number of stop bits per character.
11. From the drop-down menu, select a flow control for the serial port.
12. Click *Save* and then click *Close*. The Appliances Serial Ports window will open.
13. Click *Close*. The Unit Views window will open.

To change the CLI/console settings for a CPS or CCM appliance:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *Ports*. The Appliance Serial Ports window will open.
5. Click *CLI* in the side navigation bar. *Settings* will automatically be selected in the side navigation bar and the Appliance CLI Port Settings window will open.
6. (CPS appliances only) Using the drop-down menu, specify the appliance port you wish to use for CLI connections to a serial device. You may choose Unassigned if you do not wish to assign a specific port as the CLI port.

   Only one port may be defined as a CLI port on a CPS appliance. If a second port is defined as a CLI port, the previously defined CLI port will be changed to a standard port. For example, if Port 1 was defined as a CLI port and you now define Port 2 as a CLI port, Port 1 will become a standard port and Port 2 will be the CLI port.
7. Using the drop-down menu, specify a terminal type to use for a CLI connection.
8. Type a modem initialization string that will be used by the appliance for dial-in serial CLI access to an attached serial device. The default value is ATE0V1 SO=1.

NOTE: If you wish to access a serial device using a modem connection, you must specify PPP settings.

9. Click *Allow Connect Command on Serial CLI* to enable users to connect to another port on the appliance from the CLI/console port using the Connect command.
10. Using the drop-down menu, specify a CLI access character that will be used to access CLI mode on a serial device. The (^) character represents the **Ctrl** key. For example, specifying ^D means that pressing **Ctrl+D** will enter CLI mode.
11. Click *Disable Local Port Login* if you do not wish to require local users to log in to the local port. Local users will be recognized in the DSView software as having their preemption level set there. If this option is not selected, the local user must log in to the local port and will have a preemption level assigned to them from the DSView software or from the logged in local account.
12. Click *Save* and then click *Close*. The Unit Views window will open.

To change the PPP settings for a CPS or CCM appliance:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *Ports*. The Appliance Serial Ports window will open.
5. Click *CLI* in the side navigation bar. *Settings* will automatically be selected in the side navigation bar and the Appliance CLI Port Settings window will open.
6. Click *PPP* in the side navigation bar. The Appliance CLI PPP Settings window will open.
7. Click *PPP Enabled* to enable a modem connection to a serial device using the appliance serial CLI/console port.

   -or-

   Do not select the checkbox if you wish to use the CLI/console port with the local terminal.
8. In the Local IP Address field, type the IP address, in standard dot notation (xxx.xxx.xxx.xxx), to be used with a PPP session to the appliance.
9. In the Remote IP Address field, type the IP address, in standard dot notation (xxx.xxx.xxx.xxx), to be assigned to the PC dialing into the PPP connection on the appliance.
10. Type a subnet mask, in standard dot notation (xxx.xxx.xxx.xxx), on which both the local IP address and remote IP address must reside.
11. Click *Save* and then click *Close*. The Unit Views window will open.

To change the NFS port settings for a CCM appliance:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *Ports*. The Appliance Serial Ports window will open.
5. In the side navigation bar, select a port. Then select *NFS History File* in the side navigation bar and the Appliance NFS Port Settings window will open.
6. To enable NFS history file operations on that port, click *Enable NFS History File*.

   If you enable NFS history file operations on the port, you may optionally enter a name in the History File field. (This name is appended to the name of the mount point configured for the CCM appliance to yield a full pathname.) You may use special characters to indicate the file date; see the CCM Installer/User Guide.

Specify a 0-3584 byte threshold for writing of serial data in the Buffer Size field. If the Buffer Size and Buffer Interval values are both zero, data is written immediately. If both Buffer Size and Buffer Interval are nonzero, the first threshold that is reached will cause the write.

Specify a 0-65536 second interval for writing of serial data in the Buffer Time Interval field.

The NFS History Status area contains the current descriptive status.

7. Click *Save* and then click *Close*. The Unit Views window will open.

Displaying and changing session settings on managed appliances

The following DSView software session settings may be modified on managed appliances:

- Active - Allows a user to disconnect a managed appliance session.
- Settings - Allows settings to be specified for a DSView software session. For CPS and CCM appliances, this includes inactivity time-out and SSH settings. For DS1800 digital switches and DSR switches, this includes inactivity time-out and encryption level settings.

The following DSView software session setting may be modified on DS1800 digital switches and DSR1010, 1021, 1022, 1024, 1030, 1031, 2010, 2030, 2035, 4010, 4020, 4030, 2020, 8020, 8030 and 8035 switches only:

- Exit Macros - Allows a DSView software administrator to create macros that may be used by and reside on a DS1800 digital switch or supported DSR switches.

Customizing the Appliance Sessions window

By default, the following fields display in the Appliance Sessions window for managed appliances and may be removed by selecting the *Customize* link:

- Duration - Length of the DSView software session.
- User - Name of user who initiated the DSView software session.
- (DSR1030, 1031, 2030, 2035, 4030, 8030 and 8035 switches only) Type - Session type: KVM or Virtual Media.
- (DSR1030, 1031, 2030, 2035, 4030, 8030 and 8035 switches only) Lock Status - When there is a KVM and a virtual media session to the same target device and the appliance setting Virtual Media Locked to KVM Session is enabled, Locked will be displayed in this column.

The following fields are not displayed by default for DS1800 digital switches and DSR switches, but may be added using the *Customize* link.

- Channel - Channel being used by the managed appliance to connect to the DSView software session.
- Client - Proxy address if the proxy is enabled.
- IQ Module - EID of the target device DSRIQ or AVRIQ module. This column may also display the EID of an AVRIQ module of an AutoView 2000 switch cascaded from a DS1800 digital switch or DSR switch in a non-proxied connection.
- Mode - Mode of the session, which may change during the session. Available modes are:

  - Normal - An interactive session that may be shared with other users. When two or more users are sharing the session, the mode will change to Sharing Interactive.
  - Exclusive - A private session that does not allow sharing by other users.
  - Sharing Interactive - A DSView software session that is being shared by two or more users. Interactive users have full control of the video, mouse and keyboard. Passive users may also share the session, but may only display the session and have a mode of Sharing Passive.

    A user may display the usernames of other users sharing the session if *View identity of shared connections* is checked in the Video Viewer Session Properties dialog box or if the user is a member of the built-in administrators user group. Users viewing the session in Stealth mode will not be listed. If users disconnect from the session and a single user remains connected, the mode will change to Normal.
  - Sharing Passive - A session that is being shared by two or more users. Passive users may only display the DSView software session. Interactive users may also share the session, but have full control of the video, mouse and keyboard and have a state of Sharing Interactive.

    A user may display the usernames of other users sharing the software session if *View identity of shared connections* is checked in the Video Viewer Session Properties dialog box or if the user is a member of the built-in administrators user group. Users viewing the session in Stealth mode will not be listed. If other users disconnect from the session and a single user remains connected, the mode will change to Normal.
  - Scan - A temporary non-exclusive DSView software session that displays connected target devices in a thumbnail viewer.
- Owner - Username of the logged in user that owns the session connected to the managed appliance.
- Port - Managed appliance port number connected to the session.
- Preemption Level - Effective user preemption level for the user that is connected to the managed appliance port. See *Preemption Levels* on page 24 for more information.

The following fields are not displayed by default for CPS or CCM appliances, but may be added using the Customize link:

- Client - IP address of the DSView software client computer connected to the appliance in a non-proxied connection. The IP address of the DSView proxy will display in this column if the client is connected to the appliance using a proxy connection.
- Interface - Interface to which to the session is connected, which is either a serial port or the network CLI.
- Preemption Level - Effective user preemption level for the user that is connected to the appliance port. See *Preemption Levels* on page 24 for more information.

See *Using the Customize link in windows* on page 15 for more information.

To display session information:

NOTE: This procedure is valid on the following managed appliances: DS1800 switches, CPS appliances, CCM appliances and DSR switches.

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *Sessions*. *Active* will automatically be selected in the side navigation bar and the Appliance Sessions window will open.
5. To display information about a specific session, click on the name of the KVM, virtual media or serial session. The Active Session Information window will open, including information about the active session.
6. Click *Close*. The Appliance Sessions window will open.
7. Click *Close*. The Unit Views window will open.

To display or change the session settings on a CPS or CCM appliance:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *Sessions*. *Active* will automatically be selected in the side navigation bar and the Appliance Sessions window will open.
5. Click *Settings* in the side navigation bar. The Appliance Settings - Sessions - Settings window will open. The display includes SSH settings for the appliance.
6. Using the drop-down menu, specify the how the most recent 64K bytes of online and offline data (history) from a serial port will be controlled:
   - Auto - Select this option to display the history buffer content to a Telnet window.
   - Hold - Select this option to save the buffer contents. To display the contents, you must access the appliance CLI and issue a Port History command.
7. Click *Enable Inactivity Timeout* and use the arrows to specify a value (from 1-90 minutes) that the managed appliance will wait during inactive intervals until the session is closed and the user must log back into the managed appliance.
8. (CCM appliances only) In the Serial Session Share Mode area, enable one of the radio buttons: Disable, Auto or Query.
9. Click *Save* and then click *Close*. The Unit Views window will open.

To change the KVM session settings on a DS1800 digital switch or DSR switch:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *Sessions*. *Active* will automatically be selected in the side navigation bar and the Appliance Sessions window will open.
5. Click *Settings* in the side navigation bar and then click KVM. The Appliance KVM Session Settings window will open.
6. In the Inactivity Timeout area, click *Enable Inactivity Timeout* and use the arrows to specify a time-out value (from 1-90 minutes) that the managed appliance will wait during inactive intervals until the session is closed and the user must log back into the managed appliance.
7. In the Video Noise Compensation area, click the *Enable Video Noise Compensation* checkbox to enable this feature.
8. In the Encryption Level area, specify an encryption level for the keyboard, mouse and video:
   - DES - SSL Single DES encryption
   - 3DES - SSL Triple DES encryption
   - 128-Bit SSL - 128-bit encryption which used an ARCFOUR (RC4®) SSL cipher

   At least one encryption level must be specified for the keyboard and mouse. When you specify more than one SSL encryption type, the DS1800 digital switch or DSR switch negotiates the strongest algorithm that is supported by both sides. The strongest algorithm is 128 bit, followed by 3DES and DES.
9. Click *Save* and then click *Close*. The Unit Views window will open.

To change the virtual media session settings on a DSR switch:

NOTE: This procedure is valid on the following managed appliances: DSR1030, 1031, 2030, 2035, 4030, 8020 and 8035 switches.

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *Sessions*. *Active* will automatically be selected in the side navigation bar and the Appliance Sessions window will open.
5. Click *Settings* in the side navigation bar and then click *Virtual Media*. The Appliance Virtual Media Session Settings window will open.

6. In the Session Lock area, enable the *Virtual Media locked to KVM session* checkbox if you wish to close the virtual media session when the associated KVM session is closed. When this feature is disabled an active virtual media session will remain active when the associated KVM session is closed.
7. In the Drive Mappings area, choose an access mode from the Virtual Media Access Mode drop-down menu: read-only or read-write.

   When the access mode is read-only, the user will not be able to write data to the mapped drive on the client machine. When the access mode is read-write, the user will be able to read and write data to the mapped drive.

   If the drive is a read-only drive (for example, CD/DVD drives or ISO images), the access mode setting will be ignored. If the drive on the client machine is read-write (for example, a mass storage device or USB removal media), setting read-only access mode will prevent the user from writing data to the client machine.
8. In the Encryption Level area, enable one or more encryption levels for the virtual media session: DES, 3DES or 128-Bit SSL. Any combination of selections (or no selection) is valid.
9. Click *Save* and then click *Close*. The Unit Views window will open.

Defining exit macros

Since clients are running remotely on PCs, certain commands must be sent to the controlled target device using keyboard macros. For example, pressing **Ctrl+Alt+Delete** on your keyboard resets the PC running the client rather than resetting the target device. To reset the target device, a macro is needed. The DSView management software provides numerous sequences pre-configured for ease of operation.

Three kinds of macros are available: personal, global and exit. Personal macros and global macros are created using the Video Viewer window. See *Using Global and Personal Macros* on page 192 for more information.

Exit macros are supported on DS1800 digital switches and the following DSR switches: DSR1010, 1021, 1022, 1024, 1030, 1031, 2010, 2020, 2030, 2035, 4010, 4020, 4030, 8020, 8030 and 8035 switches.

Exit macros allow software administrators to create a macro that returns a target device to a known state. They reside on the managed appliances and are executed whenever a DSView software session is terminated. For example, if a user is connected to a target device and the user closes the Video Viewer session, an exit macro may be executed that resets the target device to a known state by logging the user out of the target device session.

Exit macros may be created and maintained by any user with Configure Unit Settings access rights. Different groups of exit macros may be created for each managed appliance in your system.

To define exit macros:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.

3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *Sessions*. *Active* will automatically be selected in the side navigation bar and the Appliance Sessions window will open.
5. Click *Exit Macros* in the side navigation bar. The Appliance Exit Macros window will open.
6. Click the number of a macro. The Appliance Exit Macro Settings window will open.
7. Enter a unique description for the global macro in the Name field.
8. From the Select Keyboard drop-down menu, select the country configuration of your keyboard. The keyboard graphic in the window will update to reflect your selection.
9. Click on the buttons in the keyboard graphic you wish to use to create the macro. As a button is clicked, it will appear in the list box to the left of the keyboard graphic.

   You may type or use the arrow buttons to specify a delay between buttons you selected from the keyboard graphic. First, click the button in the list box after which you wish to place a delay. Next, click *Delay* to insert the delay in the list box.
10. Specify the target devices on which you wish to use the macro by selecting a device in the Available list. Multiple target devices may be selected by pressing **Ctrl** while clicking on the target device names. Click *Add*. The target devices will be moved to the Assigned list.

    To remove selected target devices, select the target device from the Assigned list (multiple target devices may be selected by pressing **Ctrl** while clicking on the target device names) and clicking *Remove*. The target devices will be moved to the Available list.
11. Click *Save* and then click *Close*. The Unit Views window will open.

Example: Creating a macro where the Ctrl key is held while F1-F2-F3 are typed:

1. Type **ControlF1-F2-F3** in the Name field. This is the name of the macro that will appear in the Appliance Exit Macros window.
2. Click on the left or right *Ctrl* key in the keyboard graphic in the window. Ctrl Left - PRESS or Ctrl Right - PRESS will appear in the list box to the left of the keyboard graphic.
3. Click *F1*, *F2* and *F3* in the keyboard graphic in the window. The keystrokes will appear in the list box to the left of the keyboard graphic.
4. Click the same left or right *Ctrl* key in the graphic that you pressed in step 2. Ctrl Left - RELEASE or Ctrl Right - RELEASE will appear in the list box to the left of the keyboard graphic.
5. In the Assigned to Macro area, select the target devices to which you wish to assign the macro.
6. Click *Save* to save your changes.
7. Click *Close*.

Changing local account settings

NOTE: This procedure is valid on the following managed appliances: CPS appliances, CCM appliances and all DSR switches except the DSR800, 1161, 2161 and 4160 switches (which do not support local accounts).

Local accounts allow a user to log in to a managed appliance locally if it has a server configured as an authentication server. You may assign the user administrator, appliance administrator or user level to a local user. See *Built-in User Groups* on page 22 for more information.

To display the Appliance Local User Accounts window:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.
4. Click *Appliance Settings* in the side navigation bar and then click *Local Accounts*. The Appliance Local User Accounts window will appear.

Customizing the Appliance Local User Accounts window

By default, the following fields display in the Appliance Local User Accounts window and may be removed using the *Customize* link:

- Preemption Level - Preemption level of the local user account.
- Access Level - Access level of the local user. See *Built-in User Groups* on page 22 for information.

See *Using the Customize link in windows* on page 15 for more information.

To add a local user account:

NOTE: You must have Configure Local Accounts rights to add local user accounts.

1. From the Appliance Local User Accounts window, click *Add*. The Add Local User Account Wizard will appear. Click *Next*.
2. The Type in Local User Credentials window will open.
   a. Type the name of the local user account.
   b. Type a password for the local user account.
   c. Confirm the password for the local user account.
   d. Click *Next*.
3. The Select Preemption Level window will open. Select a preemption level (1-4) for the local user. This will be used for KVM, serial and virtual media sessions. (See *Preemption Levels* on page 24 for more information.) Click *Next*.
4. The Select Access Level window will open. Select an access level from the drop-down menu: Appliance Administrator, User or User Administrator. Then click *Next*.

DSR1010, DSR2010 and DSR4010 switches support local accounts, but the Appliance Administrator access level cannot be changed; therefore, this menu will not appear for these switches.

If you selected *User*, continue to step 5.

-or-

If you selected *Appliance Administrator* or *User Administrator*, go to step 6.

5. The Assign target devices window will open.Add or remove user access rights to a target device:

   To add user access rights to a target device, select the name of the target device in the Available Target Devices list. Multiple target devices may be selected by pressing **Ctrl** while clicking on the target devices. Click *Add*. The target devices will be moved to the Assigned Target Devices list.

   -or-

   To delete user access rights to a target device, select the name of the target device in the Assigned Target Devices list. Multiple target devices may be selected by pressing **Ctrl** while clicking on the column names. Click *Remove*. The target devices will be moved to the Available Target Devices list.

6. Click *Next*. The Completed Successful window will open.
7. Click *Finish*. The Appliance Local User Accounts window will open, including the newly-added local user.

To delete a local user account:

NOTE: You must have Configure Local Accounts rights to delete local user accounts.

1. From the Appliance Local User Accounts window:

   To delete one or more local user accounts, click the checkbox to the left of the local usernames.

   -or-

   To delete all local user accounts, click the checkbox to the left of Name at the top of the list.

2. Click *Delete*. A confirmation dialog box will appear.
3. Click *OK* to delete the local user accounts.

   -or-

   Click *Cancel* to cancel the action.

To change the settings of a local user account:

NOTE: You must have Configure Local Accounts rights specified in the Unit Access Rights window to change local user account settings.

1. From the Appliance Local User Accounts window, click on the name of a local user account. *Settings* will automatically be selected in the side navigation bar and the name of the local user

account appears under the name of the managed appliance. The Appliance Local User Account Settings window will open.

2. Type a new name for the local user.
3. Use the drop-down menu to select a preemption level (1-4) for the local user. See *Preemption Levels* on page 24 for more information.
4. If available, use the drop-down menu to select an access level: User Administrator, Appliance Administrator or User.
5. Type a new password for the local account and then confirm the password.
6. Click *Save* to save your changes.
7. Click *Close*. The Appliances window will open, including your changes.

To assign target device access rights to a local account:

NOTE: You must have Configure Appliance Local User Accounts rights to assign target device access rights to a local account.

1. From the Appliance Local User Accounts window, click on the name of a local account. *Settings* will automatically be selected in the side navigation bar and the name of the local account appears under the name of the managed appliance. The Appliance Local User Account Settings window will open.

   If the local user has Configure Local Accounts rights, a message will appear, informing you that the local user may access all target devices in the system.

   From the side navigation bar, click *Access Rights*. The Appliance Local User Account Access Rights window will open.
2. Add or remove local user account access to a target device:

   To add local user account access to a target device, select the name of the target device in the Available Target Devices list. Multiple target devices may be selected by pressing **Ctrl** while clicking on the target device name. Click *Add*. The target devices will be moved to the Assigned Target Devices list.

   To remove local user account access to a target device, select the name of the target device in the Assigned Target Devices list. Multiple target devices may be selected by pressing **Ctrl** while clicking on the target device name. Click *Remove*. The target devices will be moved to the Available Target Devices list.
3. Click *Save* to save your changes.
4. Click *Close*. The Appliance Local User Accounts window will open.

Managing Active Sessions

You may display all active connections to target devices in your DSView software system using the Active Sessions window.

Customizing the Active Sessions window

The following field is always displayed in the Active Sessions window:

- Start-Date-Time - Time when the target device session was started.

By default, the following fields display in the Active Sessions window and may be removed using the Customize link:

- Duration - Length of the DSView software session.
- User - User who initiated the session, which may be a user, a local port user or a user with a local user account.
- Target Device - Name of the target device being used for the session.
- Type - Session type, which may be KVM, Virtual Media or Serial.

The following fields are not displayed by default, but may be displayed using the Customize link:

- Client - IP address of the client computer connected to the session for a non-proxy connection. The IP address of the DSView proxy will appear in this column for a proxy connection.
- Connection - Connection path from the target device to the managed appliance. See *Managing Connections to Units* on page 132 for more information.
- Mode - Session mode, which may change during the session. Available modes are:
  - Normal - An interactive session that may be shared with other users. When two or more users are sharing the session, the mode will change to Sharing Interactive.
  - Exclusive - A private session that does not allow sharing by other users.
  - Sharing Interactive - A DSView software session that is being shared by two or more users. Interactive users have full control of the video, mouse and keyboard. Passive users may also share the software session, but may only display the session and have a mode of Sharing Passive.

    A user may display the usernames of other users sharing the DSView software session if *View identity of shared connections* is checked in the Video Viewer Session Properties dialog box or if the user is a member of the built-in administrators user group. Users viewing the session in Stealth mode will not be listed. If other users disconnect from the session and a single user remains connected, the mode will change to Normal.
  - Sharing Passive - A DSView software session that is being shared by two or more users. Passive users may only display the DSView software session. Interactive users may also share the session, but have full control of the video, mouse and keyboard and have a mode of Sharing Interactive.

    A user may display the usernames of other users sharing the session if *View identity of shared connections* is checked in the Video Viewer Session Properties dialog box or if the user is a member of the built-in administrators user group. Users viewing the session in Stealth mode will not be listed. If other users disconnect from the session and a single user remains connected, the mode will change to Normal.

  - Scan - A temporary non-exclusive DSView software session that displays connected target devices in a thumbnail viewer.
- Owner - Name of the user who launched the session, which may be a user, a local port user or a user with a local user account.
- Preemption Level - Effective user preemption level for the user that is connected to the target device session. See *Preemption Levels* on page 24 for more information.

See *Using the Customize link in windows* on page 15 for more information.

To display information about active sessions:

1. Click the *Units* tab.
2. From the side navigation bar, click *Active Sessions*. The Active Sessions window will open.
3. Click on the name of an active session in the Start-Date-Time column. The Active Session Information window will open.
4. Click *Close* to close the window and return to the Active Sessions window.

To remove an active session from the Active Sessions window:

NOTE: Removing an active session from the Active Sessions window does not disconnect the session.

1. From the Active Sessions window:

   To remove a single session from the window, click the checkbox to the left of the session.

   -or-

   To remove all active sessions from the window, click the checkbox to the left of Start-Date-Time at the top of the list.
2. Click *Remove*. A confirmation dialog box will appear.
3. Click *OK* to remove the active sessions.

   -or-

   Click *Cancel* to cancel the action.

To disconnect an active session:

NOTE: This procedure is valid on the following managed appliances: DS1800 digital switches, CPS appliances, CCM appliances and DSR switches.
A user or member of a user group may disconnect a session only if the Reboot Appliance and Disconnect Sessions unit access right is enabled for that user/user group. See *Changing Unit Access Rights* on page 102 for more information. Additionally, to disconnect a session, the user's preemption level must be higher than the preemption level of the active session user.

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The *Unit Views - Appliances - All* window will open.
3. Click on the appliance name.

4. Click *Appliance Settings* in the side navigation bar and then click *Sessions*. *Active* will automatically be selected in the side navigation bar and the Appliance Sessions window will open.
5. To disconnect one or more sessions, click the checkbox to the left of the sessions you wish to disconnect.

   -or-

   To disconnect all sessions, click the checkbox to the left of Server at the top of the list.
6. Click *Disconnect.* A confirmation dialog box will appear.

   For virtual media sessions on DSR1030, 1031, 2030, 2035, 4030, 8030 and 8035 switches only - If you attempt to disconnect an active virtual media session or a KVM session that is locked to a virtual media session, a confirmation message is displayed, indicating that any virtual media mappings will be disconnected. Click *OK* to confirm or click *Cancel*. See *Using Virtual Media* on page 200 for more information.
7. Click *OK* to confirm or click *Cancel*.

Managing Connections to Units

The *Connections* link displays either target device connections or managed appliance connections.

- The Target Device Connections window lists all connections to the target device. You may also use this window to add or delete a connection to or from the target device.
- The Appliance Connections window lists all connections from the managed appliance to cascade switches or target devices. You may rename the units which are part of the connection path through this window.

NOTE: Connections of EVR1500 environmental monitors and generic appliances may not be viewed.

Connection display format

Connections typically appear in a format similar to the following for connections to target devices, cascade switches and SPC devices:

<Managed appliance name>(<Port>) → <EID Number> → <target device>

<Managed appliance name>(<Port>) → <EID Number> → switch one <Port>→<target device>

<Managed appliance name>(<Port>) → <SPC Device> (<Port>) → <target device>

<DSI5100 Appliance Name>(<Port>)→<target device>

The following examples illustrate typical connections that may appear in your DSView software.

Example: Target device connections

In the following example, there are three target devices connected to ports 3, 4 and 8 of a DSR1021 switch named dsr-1021-huntsville. The DSR1021 switch ports are connected to the three target

devices using DSRIQ modules. The DSRIQ with an EID of 520255-044F6F is connected to target device td-john, while 520255-03F757 is connected to td-mary and 520255-016BE0 is connected to td-tim.

dsr-1021-huntsville(3)→520255-044F6F→td-john

dsr-1021-huntsville(4)→520255-03F757→td-mary

dsr-1021-huntsville(8)→520255-016BE0→td-tim

Example: Cascade switch connection

In the following example, an AutoView 200 1 x 8 switch is connected to port one of a DSR1021 switch named dsr-1021-huntsville, using a DSRIQ module with an EID of 520255-023FB7. Each port of the AutoView 200 switch is connected to a different target device (520255-023FB701 through 520255-023FB708).

dsr-1021-huntsville(1)→520255-023FB7→switch one (1)→520255-023FB701

dsr-1021-huntsville(1)→520255-023FB7→switch one (2)→520255-023FB702

dsr-1021-huntsville(1)→520255-023FB7→switch one (3)→520255-023FB703

dsr-1021-huntsville(1)→520255-023FB7→switch one (4)→520255-023FB704

dsr-1021-huntsville(1)→520255-023FB7→switch one (5)→520255-023FB705

dsr-1021-huntsville(1)→520255-023FB7→switch one (6)→520255-023FB706

dsr-1021-huntsville(1)→520255-023FB7→switch one (7)→520255-023FB707

dsr-1021-huntsville(1)→520255-023FB7→switch one (8)→520255-023FB708

Example: SPC device connection

In the following example, an SPC device is connected to the SPC port of a DSR1021 switch named dsr-1021-huntsville. SPC device outlet A1 is connected to target device 02-17-F2 SPC A1.

dsr-1021-huntsville(SPC)→02-17-F2 SPC (A1)→02-17-F2 SPC A1

Customizing the Target Device Connections window

By default, the following field displays in the Target Device Connections window and may be removed using the Customize link:

Type - Displays the type of connection:

- KVM - Connection to a port of a DS1800 digital switch or DSR switch using a DSRIQ module.
- Virtual Media - Virtual media connection.
- Serial - Serial port connection to a CPS or CCM appliance.
- Power - A connection to an SPC device outlet.
- IPMI - A connection to a DSI5100 appliance.

See *Using the Customize link in windows* on page 15 for more information.

To display a connections window:

1. In a Unit Views window, click on a unit name. *Overview* will automatically be selected in the side navigation bar and the Unit Overview window will open.
2. Click *Connections* in the side navigation bar.

   If you selected a target device, the Target Device Connections window will open, including all connections to the target device.

   -or-

   If you selected a managed appliance, the Appliance Connections window will open, including all connections to the DS1800 digital switch, DSI5100, CPS or CCM appliance or DSR switch.

To rename a managed appliance connection:

1. In the Appliance Connections window, click on a connection. The Appliance Connections - Rename window will open.
2. Type in new name for one or more items in the connection chain.
3. Click Save.
4. Click *Close*. The Appliance Connections window will open, including your changes.

Adding target device connections

To add target devices:

1. Click *Add* in the Target Device Connections window to display the Add Target Device Connection Wizard.
2. Click *Next*.
3. The Select Connection Type window will open.
   a. Select *KVM* to create a connection to a DS1800 digital switch or DSR switch port using a DSRIQ module.

      -or-

      Select *Serial* to create a serial port connection to a CPS or CCM appliance.

      -or-

      Select *Power* to create a connection to an SPC device outlet.

      -or-

      Select *IPMI* to create a connection to a DSI5100 appliance. An IPMI connection may only be made to IPMI 1.5 compatible target devices.

   b. Click *Next*.
4. The Select Appliance with Available Ports window will open. Select a managed appliance from the drop-down menu, then click *Next*.

5. The Select Available Connection window will open. Select a connection from the drop-down menu, then click *Next*.
6. The Completed Successful window will open. Click *Finish*. The Target Device Connections window will open, including the new connection to the target device.

To delete a target device connection:

1. In the Target Device Connections window, click the checkbox to the left of the target device connection you wish to delete.

   -or-

   Click the checkbox to the left of Connection at the top of the list to select all target devices listed in the window for deletion.
2. Click *Delete*. A confirmation dialog box will appear.
3. Click *OK* to delete the target device connections.

   -or-

   Click *Cancel* to cancel the action.

Unit Grouping

The DSView Explorer automatically groups managed appliances by the type of appliance (CCM1650 appliance, DS1021 switch and so on). Target devices are automatically grouped based on the type to which they are assigned.

NOTE: Recently accessed units may be viewed by clicking the *Recently Accessed* link in the side navigation bar.

You may also add and change the following types of groups:

- Personal and global unit groups - Global unit groups may be seen by all users, while personal unit groups are visible only to the user who created the group
- Custom Fields - Custom fields allow a user to create groupings of units which are accessed by all users in the DSView software system by clicking a link in the side navigation bar
- Sites
- Departments
- Locations

A site, department and location may be used together to provide a detailed description of where a unit resides. For example, a DSR1021 switch may be assigned a site of New York, a department of Information Technology and a location of Room 214.

Grouping units by site

A site is a location that contains a managed appliance. You may wish to assign a location name to a site, such as Austin, 10045 Zip Code and so on.

Sites that contain units to which a user does not have access rights will not appear in the side navigation bar.

Figure 4.3 explains how site information can be displayed.

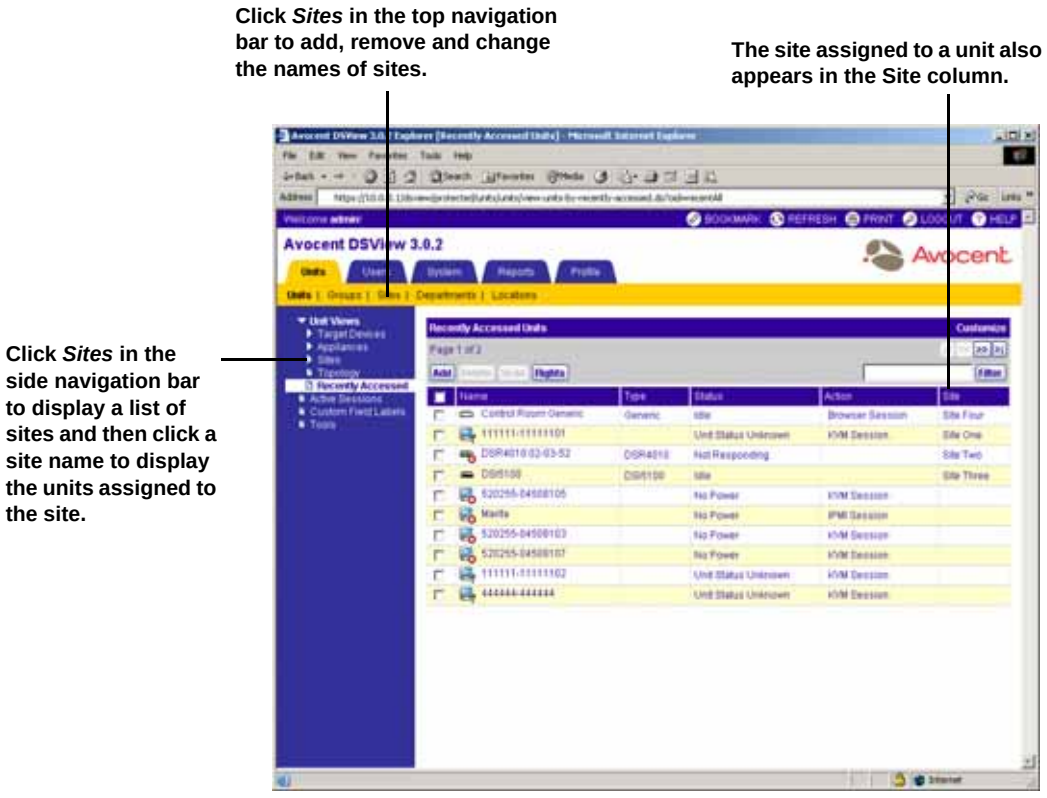

Click *Sites* in the top navigation bar to add, remove and change the names of sites.
The site assigned to a unit also appears in the Site column.
Click *Sites* in the side navigation bar to display a list of sites and then click a site name to display the units assigned to the site.
Avocent DSView 3.0.2
Avocent
Recently Accessed Units

Figure 4.3: Displaying Sites

Table 4.4 lists the windows that contain a site column.

Table 4.4: Windows Containing a Site, Department or Location Column

Window	Link Clicked in Side Navigation Bar
Units in Site	Sites
Target Devices	A link under target devices
Appliances	A link under appliances
Units in Group	Groups
Units in Custom Fields	A link under Custom Field

Table 4.4: Windows Containing a Site, Department or Location Column (Continued)

Window	Link Clicked in Side Navigation Bar
Recently Access Units	Recently Accessed
Topology	Topology

To display the Sites window:

1. Click *Units* in the tab bar.
2. Click *Sites* in the side navigation bar. *Sites* will automatically be selected in the side navigation bar and the Sites window will open.

To add a site:

1. In the Sites window, click *Add*. The Add Site window will open.
2. Type a name for the site.
3. Click *Add*. The Sites window will open including the newly added site.

To delete a site:

1. In the Sites window:

   To delete one or more sites, click the checkbox to the left of the sites.

   -or-

   To delete all sites in the window, click the checkbox to the left of Name at the top of the list.
2. Click *Delete*. A confirmation dialog box will appear.
3. Click *Yes* to delete the sites.

   -or-

   Click *No* to cancel the action.

To change the name of a site:

1. In the Sites window, click on the name of a site. The side navigation bar will change to include the name of the site at the top.
2. Click *Name*. The Site Name window will open.
3. Type a new 1-64 character name in the Name field.
4. Click *Save* to save your changes and then click *Close*. The Sites window will open including the renamed site.

To display the units associated with a site:

1. Click *Units* in the tab bar. *Units* will automatically be selected in the top navigation bar.
2. Click *Sites* in the side navigation bar. The Units in Site window will open with information for the first alphabetically-listed site.

3. Click on a site link in the side navigation bar to display another site.

To associate or change the association of an existing unit to a site:

1. Click *Units* in the tab bar. *Units* will automatically be selected in the top navigation bar.
2. Click one of the links listed in Table 4.5 in the side navigation bar to display the corresponding window for the units you wish to associate, change or remove the association.

Table 4.5: Links for Adding, Changing or Removing Site, Department or Location Association

Link	Window	Changes Site Associations For
A link under Target Devices	Target Devices	Target devices only
A link under Appliances	Appliances	Managed appliances only
Sites	Units in Site	Units
Groups	Units in Group	Units
A link under Custom Field	Units in Custom Fields	Units
Recently Accessed	Recently Accessed Units	Units
Topology	Topology	Units

NOTE: For custom fields to display in the side navigation bar, at least one unit to which a user has access rights must have a custom field setting. The default labels for custom fields defaults are Custom Field 1, Custom Field 2 and Custom Field 3, which may be changed. See *Managing units by custom fields* on page 144 for more information.

3. Click on the name of a unit. The Unit Overview window will open.
4. Click *Properties* in the side navigation bar, then click *Location*.
5. Using the drop-down menu, select the site to associate with the unit. If you do not wish to associate the unit with any site, choose the top (empty) item from the drop-down menu.
6. Click *Save* and then click *Close*. The Site column will display the new site name and the unit will appear under the site when you click *Units* from the tab bar and *Sites* and the site name from the side navigation bar.

Grouping units by department

A department is a location name used to identify where a unit resides, and may be named anything you wish. For example, you may wish to assign department names such as Software Development, Human Resources, Accounting and so on.

The department assigned to a unit may appear in the Department column of the windows listed in Table 4.4 in a Units view. By default, the Department column is not displayed in any of the windows, but you may add it by using the window's Customize link. See *Using the Customize link in windows* on page 15 for more information.

To use a department:

1. Add the department.
2. Associate units with the department.

To display the Departments window:

1. Click *Units* in the tab bar.
2. Click *Departments* in the top navigation bar. *Departments* will automatically be selected in the side navigation bar and the Departments window will open.

To add a department:

1. In the Departments window, click *Add*. The Add Department window will open.
2. Type a name for the department. Department names may be 1-64 characters long.
3. Click *Add*. The Departments window will open, including the newly added department.

To delete a department:

1. In the Departments window:

   To delete one or more departments, click the checkbox to the left of the departments.

   -or-

   To delete all the departments in the window, click the checkbox to the left of Name at the top of the list.
2. Click *Delete*. A confirmation dialog box will appear.
3. Click *Yes* to confirm or *No* to cancel.

To change the name of a department:

1. In the Departments window, click on the name of a department. The side navigation bar will change to include the name of the department at the top.
2. Click *Name*. The Department Name window will open.
3. Type a new 1-64 character name in the Name field.
4. Click *Save* and then click *Close*. The Departments window will open, including the renamed department.

To associate or change the association of an existing unit to a department:

1. Click *Units* in the tab bar.
2. Click one of the links listed in Table 4.5 in the side navigation bar to display the corresponding window for the units you wish to associate, change or remove the association.
3. Click on the name of a unit. The Unit Overview window will open.
4. Click *Properties* in the side navigation bar and then click *Location*.

5. Using the drop-down menu, select the department to associate with the unit. If you do not wish to associate the unit with any department, choose the top (empty) item from the drop-down menu.
6. Click *Save* and then click *Close*. The Department column will display the new department name.

Grouping units by location

A location may be named anything you wish. For example, you may wish to assign location names such as Lab Room 101, System Administrator's Office and so on.

The location assigned to a unit will appear in the Location column of the windows listed in Table 4.4 in a Units view. By default, the Location column is not displayed in any of the windows, but you may add it using the window's Customize link. See *Using the Customize link in windows* on page 15 for more information.

To use a location:

1. Add the location.
2. Associate units with the location.

To display the Locations window and display locations:

1. Click *Units* in the tab bar.
2. Click *Locations* in the top navigation bar. *Locations* will automatically be selected in the side navigation bar and the Locations window will open.

To add a location:

1. In the Locations window, click *Add*. The Add Location window will open.
2. Type a name for the location.
3. Click *Add*. The Locations window will open, including the newly added location.

To delete a location:

1. In the Locations window:

   To delete one or more locations, click the checkbox to the left of the locations.

   -or-

   To delete all locations in the window, click the checkbox to the left of Name at the top of the list.
2. Click *Delete*. A confirmation dialog box will appear.
3. Click *Yes* to confirm or *No* to cancel.

To change the name of a location:

1. In the Locations window, click on the name of a location. The side navigation bar will change to include the name of the location at the top.

2. Click *Name*. The Location Name window will open.
3. Type a new 1-64 character name in the Name field.
4. Click *Save* and then click *Close*. The Locations window will open including the renamed location.

To associate or change the association of an existing unit to a location:

1. Click *Units* in the tab bar.
2. Click one of the links listed in Table 4.5 in the side navigation bar to display the corresponding window for the units you wish to associate, change or remove the association.
3. Click on the name of a unit. The Unit Overview window will open.
4. Click *Properties* in the side navigation bar and then click *Location*.
5. Using the drop-down menu, select the location to associate with the unit. If you do not wish to associate the unit with any location, choose the top (empty) item from the drop-down menu.
6. Click *Save* and then click *Close*. The Location column will display the new location name.

Grouping units by unit group

Unit groups may be used to organize units There are two types of unit groups:

- Personal - A personal unit group may only be viewed by the user who created it. Up to 32 personal unit groups may be created by a user.
- Global - A global unit group may be viewed by any user logged in to the DSView software.

Personal unit groups will appear in the Personal Unit Groups window and global unit groups will appear in the Global Unit Groups window. You may specify the number of unit groups that display in each window by using the *Customize* link. See *Using the Customize link in windows* on page 15 for more information.

Units may belong to multiple groups. For example, you may have a DSR1021 switch that belongs to two global groups and three personal groups.

You may add and remove the unit access rights for a unit group. See *Changing Unit Access Rights* on page 102 for more information.

To display unit groups:

1. Click *Units* in the tab bar.
2. Click *Groups* in the top navigation bar. *Personal* will automatically be selected in the side navigation bar and the Personal Unit Groups window will open.

   -or-

   Click *Global* in the side navigation bar. The Global Unit Groups window will open.

To add a unit group:

NOTE: Global unit groups may only be created by users with DSView software administrator, user administrator or appliance administrator privileges.

1. In the Global Unit Groups or Personal Unit Groups window, click *Add*. The Add Unit Group wizard will appear. Click *Next*.

   If you are a member of the DSView software administrators, user administrators or appliance administrators built-in user groups, continue to step 2.

   -or-

   If you are a member of any other user group, go to step 3.
2. The Select Unit Group Type window will open.
   a. Select *Personal Unit Groups* from the drop-down menu to create a personal unit group.

      -or-

      Select *Global Unit Groups* from the drop-down menu to create a global unit group.
   b. Click *Next*.
3. The Type in Unit Group Name window will open. Type a name for the unit group and then click *Next*.
4. The Completed Successful window will open. Click *Finish*. The Personal Unit Groups or Global Unit Groups window will open, including the newly added unit group.

To delete a unit group:

NOTE: You may delete global or personal unit groups. Deleting a group deletes the group only. The units still exist in the DSView software system. Global unit groups may only be deleted by users with DSView software administrator, user administrator or appliance administrator privileges.

1. In the Global Unit Groups or Personal Unit Groups window:

   To delete one or more unit groups: click the checkbox to the left of the unit groups.

   -or-

   To delete all unit groups in the window, click the checkbox to the left of Name at the top of the list.
2. Click *Delete*. A confirmation dialog box will appear.
3. Click *Yes* to confirm or *No* to cancel.

To change the name of a unit group:

NOTE: Global unit group properties may only be modified by users with administrator, user administrator or appliance administrator privileges.

1. In the Global Unit Groups or Personal Unit Groups window, click on the name of a unit group. *Name* will automatically be selected in the side navigation bar and the Unit Group Name window will open. The side navigation bar will include the name of the unit group at the top.
2. Type a new 1-64 character name in the Group field.
3. Click *Save* and then click *Close*. The Personal Unit Groups or Global Unit Groups window will open, including the renamed unit group.

To add or remove unit group members:

NOTE: Removing a unit from a global or personal unit group does not delete the unit from the DSView software system or any other group to which it belongs. Members may only be added to global unit group properties by users with administrator, user administrator or appliance administrator privileges.

1. In the Global Unit Groups or Personal Unit Groups window, click on the name of a unit group. *Name* will automatically be selected in the side navigation bar and the Unit Group Name window will open. The side navigation bar will include the name of the unit group at the top.
2. Click *Members* in the side navigation bar. The Unit Group Members - <Group Name> window displays a list of all units belonging to the unit group.
3. Click *Assign*. The Assign Units to Unit Group window will open.
4. To add a unit to the unit group:
   a. Select the unit you wish to add from the Available Units list. Multiple units may be selected by pressing **Ctrl** while clicking on the unit names.
   b. Click *Add*. The units will be moved to the Units to Assign list.

   -or-

   To remove a unit already assigned to the unit group:
   a. Select the unit you wish to remove from the Units to Assign list. Multiple units may be selected by pressing **Ctrl** while clicking on the unit names.
   b. Click *Remove*. The units will be moved to the Available Units list.
5. Click *Save* and then click *Close*. The Unit Group Members window will open, including your additions or removals.
6. Click *Close*. The Personal Unit Groups or Global Unit Groups window will open.

Using groups to display and change units

You may change the fields that display in the Units in Group window by clicking on the *Customize* link. See *Using the Customize link in windows* on page 15 for more information.

The Units in Group window allows you to delete, scan and assign rights to all or specific units in a personal or global group.

NOTE: If a personal or global group does not contain at least one unit, the group will not display in the side navigation bar.

The side navigation bar links in this window work identically to those selected from a Unit Views window. See *Managing Units* on page 95 for more information.

To display a personal or global group in the Units in Group window:

1. Click *Units* in the tab bar.
2. Click *Groups* in the side navigation bar. The Units in Group window will open and display the first alphabetically-listed personal or global group.

3. In the side navigation bar, click on the name of the personal or global group you wish to view. A Units in Group window will open, containing only the units that have been added to the group.

Managing units by custom fields

Three custom fields are available. You may change the default custom field labels (Custom Field 1, Custom Field 2 and Custom Field 3) and then associate units to the custom fields.

Figure 4.4 illustrates the custom field feature.

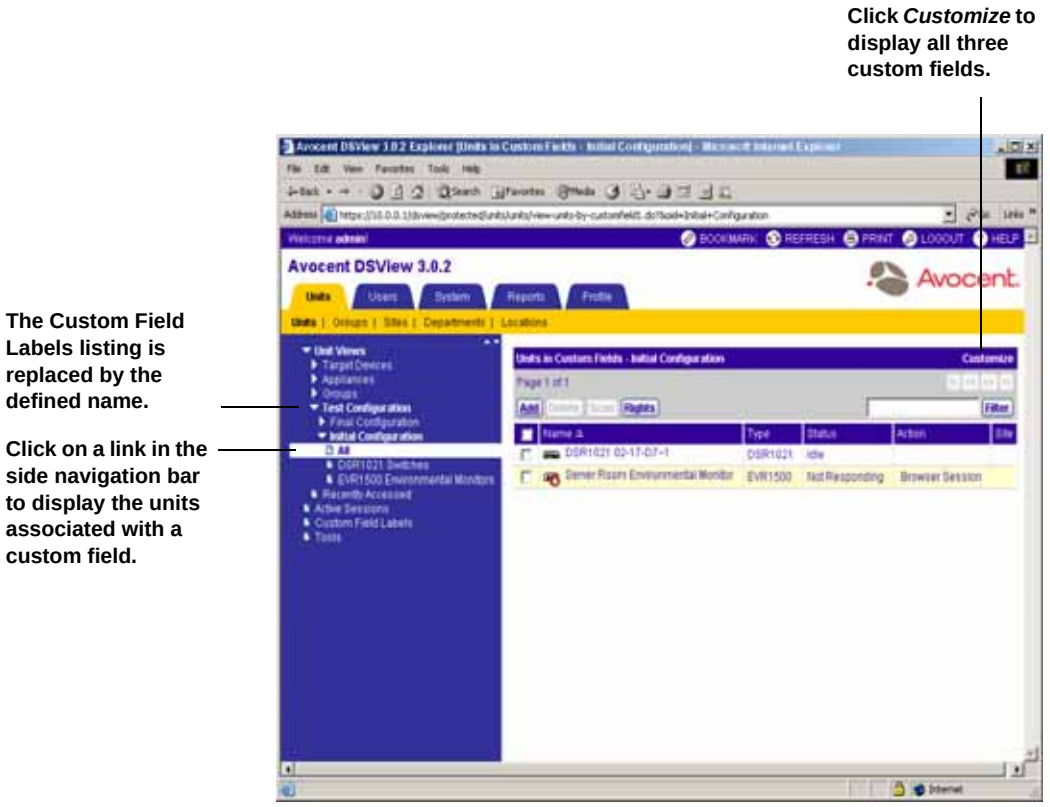

Click *Customize* to display all three custom fields.
The Custom Field Labels listing is replaced by the defined name.
Click on a link in the side navigation bar to display the units associated with a custom field.
Avocent DSView 3.0.2
Units in Custom Fields - Initial Configuration
Customize

Figure 4.4: Units in Custom Field Window

To define custom fields:

NOTE: You must have Software Administrator or Appliance Administrator access to define custom fields.

1. Click *Units* in the tab bar.
2. Click *Custom Field Labels* in the side navigation bar. The Unit Custom Field Labels window will open.

3. In Label 1, type the 1-64 character name for the first custom field label. All first-level custom fields for units will appear under this heading in the side navigation bar.
4. In Label 2, type the 1-64 character name for the second custom field label. All second-level custom fields for units will appear under this heading in the side navigation bar.
5. In Label 3, type the 1-64 character name for the third custom field label. This custom field will not appear in the side navigation bar, but may be displayed in the content area by clicking *Customize* and adding the field.
6. Click *Save* to save your changes.

Custom Field Labels will continue to appear in the side navigation bar until you associate the custom label with a unit.

To associate a custom label with a unit:

1. Click *Units* in the tab bar.
2. Click *Appliances* in the side navigation bar. The Appliances - All window will open.
3. Click on a unit. The Unit Overview window will open. The side navigation bar will include the name of the unit at the top and a list of links below it.
4. Click *Properties* in the side navigation bar and then click *Custom Fields*. The Unit Custom Fields window will open, including the custom field names.
5. In the first field, type the 1-64 character name to associate with the first label defined for the DSView software system. You may also leave the field blank.
6. In the second field, type the 1-64 character name to associate with the second label defined for the DSView software system. You may also leave the field blank.
7. In the third field, type the 1-64 character name to associate with the third label defined for the DSView software system. You may also leave the field blank.
8. Click *Save* and then click *Close*. The Appliance - All window will open. The side navigation bar will include the names of the defined and associated custom fields.

NOTE: The first, second and third custom fields may be displayed in the content area by clicking *Customize* and turning them on.

Custom fields example

In the following example, a DSView software administrator wishes to examine a test configuration of units. The units will be placed in one of two groups: an initial configuration group or a final configuration grouping. The software administrator also wishes to identify the managers of the units. At the present time, the DSView software administrator has one DSR1021 switch and one EVR1500 environmental monitor to add to the test configuration group and one generic appliance to add to the final configuration group.

1. First, the DSView software administrator will define the custom fields.
    a. Click *Units* in the tab bar.

b. Click *Custom Field Labels* in the side navigation bar. The Unit Custom Field Labels window will open.

c. In Label 1, type **Test Configuration**. All first-level custom fields for units will appear under this heading in the side navigation bar.

d. In Label 2, type **Appliances and target devices**. All second-level custom fields for units will appear under this heading in the side navigation bar.

e. In Label 3, type **Manager**. This custom field will not appear in the side navigation bar, but may be displayed in the content area by clicking *Customize* and adding the field.

f. Click *Save* to save your changes.

Custom Field Labels will still appear in the side navigation bar because the administrator has not yet defined any custom fields for units.

2. A DSR1021 switch has been configured on the system, but will need to go into a group named Initial Configuration, since it has not yet been verified for the final configuration. The administrator will associate the DSR1021 switch managed by John Smith to the custom fields as follows:

a. Click *Appliances* in the side navigation bar. The Appliances - All window will open.

b. Click on a DSR1021 switch. The Unit Overview window will open. The side navigation bar will include the name of the DSR1021 switch at the top and a list of items below it.

c. Click *Properties* in the side navigation bar and then click *Custom Fields*. The Unit Custom Fields window will open, including the custom field names you defined in step 1.

d. In the Test Configuration field, type **Initial Configuration**.

e. In the Appliances and target devices field, type **DSR1021 Switches**.

f. In the Manager field, type **John Smith**.

g. Click *Save* and then click *Close*. The Appliance - All window will open. The side navigation bar will now include Test Configuration instead of Custom Field Labels.

3. The test configuration will also include an EVR1500 environmental monitor that is managed by Mary Jones. The EVR1500 environmental monitor has also not been verified for the final configuration, so the administrator will include it in the Initial Configuration group.

a. In the Appliances - All window, click on an EVR1500 environmental monitor. The Unit Overview window will open. The side navigation bar will include the name of the EVR1500 environmental monitor at the top and a list of items below it.

b. Click *Properties* in the side navigation bar and then click *Custom Fields*. The Unit Custom Fields window will open, including the custom field names you defined in step 1.

c. In the Test Configuration field, type **Initial Configuration**.

d. In the Appliances and target devices field, type **EVR1500 Environmental Monitors**.

e. In the Manager field, type **Mary Jones**.

f. Click *Save* and then click *Close*. The Appliance - All window will open.

4. The configuration of a generic appliance has been verified, so the administrator now wishes to create a group named Final Configuration that will contain the final test units. The group will contain one generic appliance managed by Tim Brown.
   a. In the Appliances - All window, click on a generic appliance. The Unit Overview window will open. The side navigation bar will include the name of the generic appliance at the top and a list of items below it.
   b. Click *Properties* in the side navigation bar and then click *Custom Fields*. The Unit Custom Fields window will open, including the custom field names you defined in step 1.
   c. In the Test Configuration field, type **Final Configuration**.
   d. In the Appliances and target devices field, type **Generic Appliances**.
   e. In the DSView software users field, type **Tim Brown**.
   f. Click *Save* and then click *Close*. The Appliance - All window will open.

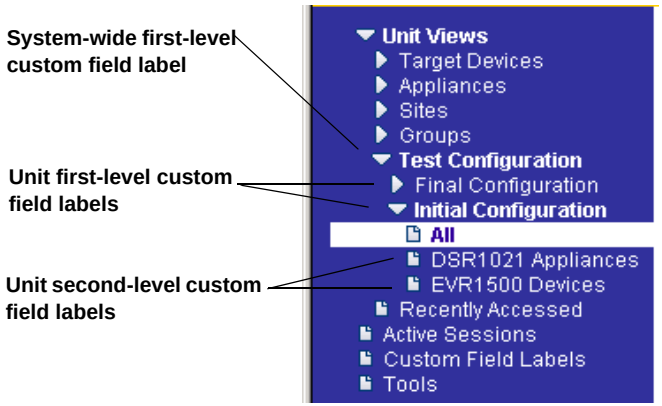


Figure 4.5: Custom Fields Example: Side Navigation Bar

CHAPTER 5

Managing User Accounts

The DSView software allows you to:

- Add, change and delete user accounts
- Unlock user accounts
- Specify user account restrictions
- Change user group membership
- Display user and user group access rights to target devices and managed appliances
- Add and delete user-defined user groups
- Display, assign and remove user group members from built-in or user-defined user groups

About the User Accounts Windows

User accounts are displayed and managed through the User Accounts windows. Figure 5.1 shows a User Accounts - All window.

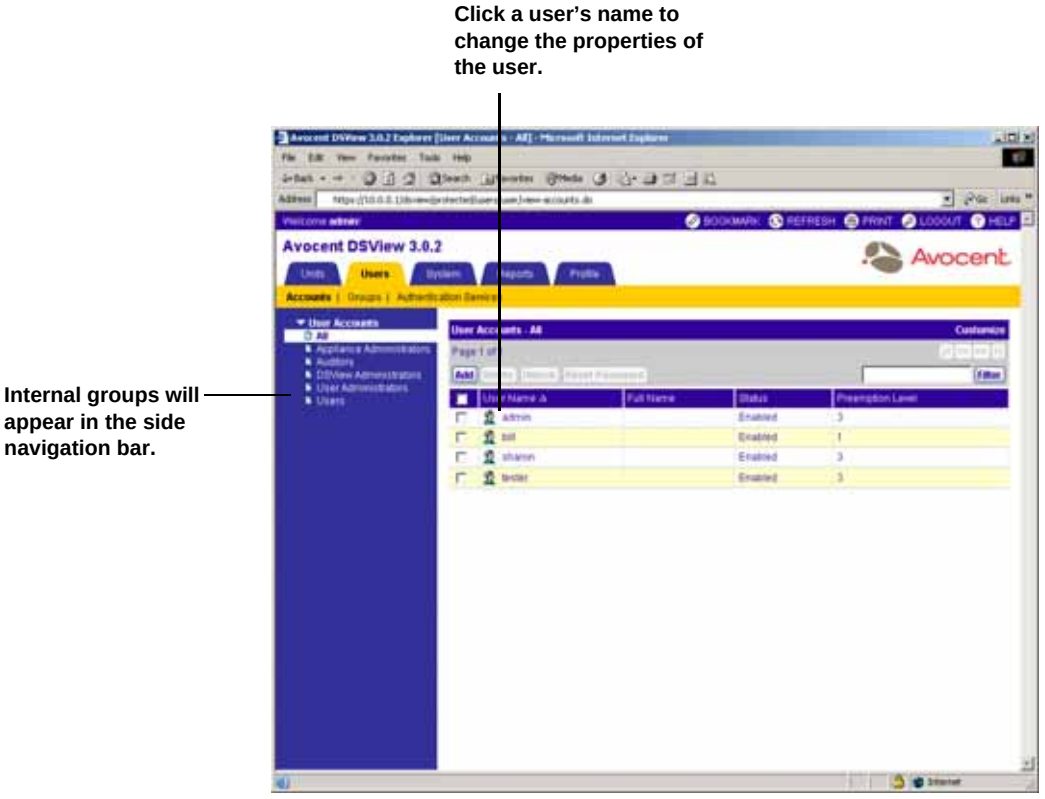

Click a user's name to change the properties of the user.
Internal groups will appear in the side navigation bar.
Avocent DSView 3.0.2
Avocent

Figure 5.1: User Accounts - All Window

Clicking on one of the links under User Accounts in the side navigation bar will display a User Accounts window containing a list of all users belonging to the particular type of user account. For example, if three users named John, Mary and Tim are members of the appliance administrators built-in user group, clicking *Appliance Administrators* in the side navigation bar will display these three as well as other users that are members of the appliance administrators built-in user group.

NOTE: A user may belong to multiple user groups.

There are five predefined user groups that appear in the side navigation bar: Appliance Administrators, Auditors, DSView software administrators, User Administrators and Users. These user groups' privileges may not be changed. See *Managing User Groups* on page 163 for more information. You may also create user-defined groups, which will also appear in the side navigation bar.

The properties of a user account may be modified by clicking on a user's name. Links for items that may be modified will appear in the side navigation bar. See *Changing User Account Properties* on page 155 for more information.

To display the User Accounts window:

1. Click the *Users* tab. *Accounts* will automatically be selected in the top navigation bar, *User Accounts - All* will automatically be selected in the side navigation bar and the User Accounts - All window will open including all users in your DSView software system.

   By default, the User Accounts - All window includes a Preemption Level column. When the window contains this column or a Group Preemption Level column, values are not displayed for external users (users validated with external authentication services). You may display an external user's effective and group preemption level by selecting the user's name from the side navigation bar and then selecting *Preemption Levels*.
2. Click one of the links below User Accounts in the side navigation bar to display the User Accounts window you wish to view.

Customizing the User Accounts window

By default, the User Name field is always displayed in the User Accounts window. One of the icons in Table 5.1 will appear to the left of the usernames and represent the status of each DSView software user.

Table 5.1: User Status Icons

Icon	Assigned Authentication Method	Description
	Internal	Disabled - The user cannot log in to the DSView software. See *Specifying user account restrictions* on page 158 for more information.
	All	Enabled - The user can log in and use the DSView software.
	Internal	Locked - The user account has been locked and the user cannot log in to the DSView software because the maximum number of log in failures has been exceeded. See *Managing Authentication Services* on page 58 and *Unlocking User Accounts* on page 155 for more information.
	All external services	Suspicious - The user account exists for the user, but the external authentication server no longer contains the account.

The following fields display in the User Accounts window and may be removed by clicking the *Customize* link:

- Full Name - Displays another name for a user-defined in the user's properties. For example, a user may have a username of Sunrise1 and a full name defined as Mary Jones. See *Changing usernames* on page 156 for more information.

- Status- Displays whether the user account is Enabled, Disabled, Locked or Suspicious. One of the icons in Table 5.1 will appear to the left of the user in the User Name column, reflecting the status of the user account.
- Preemption Level - Displays the effective preemption level of a user. See *Preemption Levels* on page 24 for more information.

The following fields may be displayed in the User Accounts window by clicking the *Customize* link:

- Authentication Server - Displays the name of the internal or external authentication server. See *Managing Authentication Services* on page 58 for more information.
- Business Address - Displays the business address defined in the user's properties. See *Specifying user address information* on page 159 for more information.
- Business Mobile - Displays the business mobile phone number defined in the user's properties. See *Specifying user phone contact information* on page 160 for more information.
- Business Phone - Displays the business phone number defined in the user's properties. See *Specifying user phone contact information* on page 160 for more information.
- Default E-Mail - Displays the default email account defined in the user's properties. See *Specifying email contact information for users* on page 160 for more information.
- Custom Field 1-Custom Field 6 - Displays the custom fields for the user. If you have specified text for a custom field, that text will display when you display the custom field. See *Managing User Groups* on page 163 for more information.
- E-Mail 1-E-Mail 5 - Displays five additional email accounts defined in the user's properties. See *Specifying email contact information for users* on page 160 for more information.
- Group Preemption Level - Displays the highest preemption level of all groups to which the user belongs. For example, if a user belongs to appliance administrators (with a group preemption level of 3) and auditors (with a group preemption level of 1), this field will display 3. See *Preemption Levels* on page 24 for more information.
- Home Address - Displays the home address defined in the user's properties. See *Specifying user address information* on page 159 for more information.
- Home Phone - Displays the home phone number defined in the user's properties. See *Specifying user phone contact information* on page 160 for more information.
- Mobile Phone - Displays the mobile phone number defined in the user's properties. See *Specifying user phone contact information* on page 160 for more information.
- Pager - Displays the pager number defined in the user's properties. See *Specifying user phone contact information* on page 160 for more information.
- User Preemption Level - Displays the user preemption level defined in the user's properties. See *Preemption Levels* on page 24 and *Changing the preemption level for a user* on page 159 for more information.

See *Using the Customize link in windows* on page 15 for more information.

Adding User Accounts

The following information is configured when a user account is created:

- Whether the user will be authenticated using the DSView internal authentication or an external authentication server.
- The user groups in which the user will be included. Each user group contains specific access rights that allow a user to perform specific actions.
- The preemption level for interrupting or disconnecting serial or KVM sessions. See *Preemption Levels* on page 24 for more information.

NOTE: You must have DSView software administrator or user administrator rights to add a user. See *Managing User Groups* on page 163 for more information.

To add a user account:

1. In a User Accounts window, click the *Add* button. The Add User Account Wizard will appear. Click *Next*.
2. The Select Authentication Service window will open.

   This window lists all external authentication servers and the DSView Internal server that may be used to authenticate users when they log in. See *Managing Authentication Services* on page 58 for more information.

   a. Select an authentication service.

   b. Click *Next*.

   If you selected *DSView Internal* as the authentication service, continue to step 3.

   If you selected *RADIUS* or *TACACS+* as the authentication service, continue to step 4.

   If you selected any other type of authentication service, continue to step 5.
3. The Type in User Credentials window will open.

   a. Type a username, password and confirm the password of the user you are adding. To enable users to set their own passwords when they log in to the DSView software, click *User must change password at next login*.

   Usernames may contain up to 64 non-case sensitive characters. Usernames are case-preserving. For example, if an account named JDoe is created, it will be saved as JDoe in the DSView software server, but a user may log in as JDoe, jdoe, JDOe and so on.

   Passwords may contain 3-64 characters. Passwords will never expire unless *User must change password at next login* is selected in the Unit Password window, or Passwords Expire information is specified in the Authentication Service User Account Policies window. A DSView software administrator may specify a different minimum character length and change expiration criteria. See *Managing Authentication Services* on page 58 for more information.

   b. Click *Next*. Go to step 6.

4. The Specify User Name window will open. Type the username on the RADIUS or TACACS+ server (74 UTF-8 characters as recommended in RFC 2865), then click *Next*. Continue to step 7.
5. Click *Specify user on external authentication service* and type the name of the user in the field. Usernames may contain up to 64 characters. Usernames may or may not be case sensitive, depending on the requirements of your external authentication server.

   -or-

   Click *Find user on external authentication service* to browse a list of users on the external authentication service.

   Click *Next*.

   If you selected *Find user on external authentication service*, continue to step 6.

   If you selected *Specify user on external authentication service*, continue to step 7.
6. The Select User from External Authentication Service window displays. If the list of users contains more than 5000 entries, a message will indicate that not all items are displayed.
   a. Select a user from the list. You may filter the list by using the Filter button and the adjacent text field. Specifying a username in the text field will return all valid matches. If filtering on another item (such as full name), you must include a wildcard. See *Filtering information in a window* on page 13 for more information.
   b. Click *Next*.
7. The Assign User to User Groups window will open. This window displays a list of all built-in groups and any user-defined groups in the authentication service you specified for the user.
   a. Select one or more groups from the Available Groups window and click *Add* to make the user a member of the groups.
   b. Click *Next*.
8. The Select User Preemption Level window will open.
   a. Type a preemption level (from 1-4) in the field, or select it using the drop-down menu. The higher the number, the higher the preemption level. For example, a user with a preemption level of 4 can preempt users assigned preemption levels of 1, 2 or 3. See *Preemption Levels* on page 24 for more information.
   b. Click *Next*.
9. The Completed Successful window will open. Click *Finish*. The user has been added.

NOTE: The DSView software obtains external group membership and external user information when a user logs in. If a user's group membership changes or the user is deleted externally, the DSView software will not see those changes until the next time that user logs in.

Deleting User Accounts

To delete user accounts:

1. In a User Accounts window, click the checkbox to the left of the users you wish to delete.

   -or-

   Click the checkbox to the left of User Name at the top of the list to select all users listed in the window for deletion.
2. Click *Delete*. A confirmation dialog box will appear.
3. Click *Yes* to confirm or *No* to cancel.

Unlocking User Accounts

If lock-out settings have been specified for the DSView internal authentication service and a user exceeds these settings, the user will not be allowed to attempt another log in until a certain amount of time has passed. Users that have been locked out will appear with a lock next to their name in the User Accounts window and *Locked* will appear in the Status column.

User administrators or administrators may manually unlock the user accounts. See *Managing Authentication Services* on page 58 for more information.

To unlock a user account:

1. In a User Accounts window, click the checkbox to the left of the users you wish to unlock.
2. Click *Unlock*. The specified users' accounts will be unlocked and the User Accounts - All window will update.

Resetting a User Account Password

A DSView software administrator or user administrator may choose to reset a user's password. The user will be required to login by typing **password** as their password and then choosing and verifying a new password for their account the next time they wish to start a new DSView management software session.

To reset a user account password:

1. In a User Accounts window, click the checkbox to the left of the user(s) to reset the password.
2. Click *Reset Password*.
3. A confirmation message box will appear. Click *Yes* to reset the password for the user or *No* to cancel.

Changing User Account Properties

If you have DSView software administrator or user administrator privileges, you may change the following account properties for a user:

- The user (login) name and full name
- The certificate associated with the user
- The SSH key associated with the user
- Login password
- Account login restrictions
- The user groups to which the user is assigned
- User preemption levels
- Home and business addresses
- Home, business, mobile and pager phone numbers
- Primary email address and up to five additional email addresses
- Notes you wish to add about the user
- Up to six custom fields

To change a user account:

1. Click on the name of a user in a User Accounts window. The name of the user account will appear at the top of the side navigation bar and a list of links will appear beneath the name.
2. Click on a link to display a window in which you may change the specific property.

Changing usernames

The username information that you may specify for a user includes:

- User Name - The name that the DSView software uses to log in and identify the user.
- Full Name - The actual name of the user.

For example, you may use Engr10 as the username and Jonathan Z. Smith as the full name to identify the person associated with the username of a user in a User Accounts window.

To change the name of a user:

1. In a User Accounts window, click on a username. *Name* will automatically be selected in the side navigation bar and the User Name window will open.
2. Type the username for the user.
3. Type the full name of the user.
4. Click *Save* and then click *Close*. The User Accounts window will open including any changes.

Changing certificates associated with users

NOTE: This property may only be modified for users using internal authentication. See *Managing Authentication Services* on page 58 for more information.

As an alternative to using this method, the user may change the certificate in the profile settings, but only if the administrator has enabled a global setting to allow it. See *Specifying a user certificate* on page 21 for more information.

To change the certificate associated with a user:

1. In a User Accounts window, click on a username. *Name* will automatically be selected in the side navigation bar and the User Name window will open.
2. Click *Credentials* in the side navigation bar and then click *Certificate*. The User Certificate window will open.
3. Type the path and name of the certificate or use the *Browse* button and select a certificate using the Choose File dialog box.
4. Click *Save* and then click *Close*. The User Accounts window will open including any changes.

Specifying a user SSH key

A configurable SSH key may be used by a CCM appliance to authenticate a DSView software user who is using an out of band client (for example, someone using a Putty SSH client that was not started by DSView software). The user supplies the public/private SSH key when connecting to the CCM appliance (only RSA keys with a maximum length of 1024 bits are allowed).The appliance then verifies the public key against the one stored for the user in the DSView software.

As an alternative to using this method, the user may specify the SSH key in the profile settings, but only if the administrator has enabled a global setting to allow it. See *Specifying an SSH key* on page 22 for more information.

To specify a user SSH key:

1. In a User Accounts window, click on a username. *Name* will automatically be selected in the side navigation bar and the User Name window will open.
2. Click *Credentials* in the side navigation bar and then click *SSH Key*. The User SSH Key window will open.
3. Type the 1-256 character name of the file containing the public SSH key that was generated by a third party key generator.

   -or-

   Click the *Browse* button and select a certificate using the Choose File dialog box.
4. Click *Save* and then click *Close*. The User Accounts window will open, including any modifications. The SSH key file will be uploaded to the DSView software server for use in authenticating the user.

Changing user passwords

NOTE: This property may only be modified for users using internal authentication. See *Managing Authentication Services* on page 58 for more information.

The password of a user may be changed or you may specify that the users enter a new password when they log in to their next session.

To change the password of a user:

1. In a User Accounts window, click on a username. *Name* will automatically be selected in the side navigation bar and the User Name window will open.
2. Click *Password* in the side navigation bar. The User Password window will open.
3. Type the new password you wish to assign to the user and verify the password.
4. Click *User must change password at next login* to enable a user to define a new password when they log in to their next session.
5. Click *Save* and then click *Close*. The User Accounts window will open, including any changes.

Specifying user account restrictions

NOTE: This property may only be modified for users using internal authentication. See *Managing Authentication Services* on page 58 for more information.

To specify account restrictions for users:

1. In a User Accounts window, click on a username. *Name* will automatically be selected in the side navigation bar and the User Name window will open.
2. Click *Restrictions* in the side navigation bar.The User Account Restrictions window will appear.
3. Click *Disable user account* to prevent the user from logging in to the DSView management software. The user's account may be re-enabled by unchecking *Disable user account*.

NOTE: The users will remain logged in if they have an open session.

4. Click *User must change password at next login* to enable a user to define a new password when logging in to the session.
5. Click *User cannot change password* to prevent the user from changing a password.
6. Click *Password never expires* to prevent a user's password from expiring.
7. Click *Save* and then click *Close*. The User Accounts window will open including any changes.

Changing user group membership

The DSView software enables you to add and remove users from user groups.

To change the group membership of a user:

1. In a User Accounts window, click on a username. *Name* will automatically be selected in the side navigation bar and the User Name window will open.
2. Click *User Groups* in the side navigation bar. The User Group Membership window will open.
3. Select the groups to which you wish to add or remove a user.

   To add a user to one or more groups:

a. In the Available Groups list, select the group to which you wish to add a user. Multiple groups may be selected by pressing **Ctrl** or **Shift** while clicking on the group names.

b. Click *Add*. The columns will be moved to the Member of list.

-or-

To remove the user from one or more groups:

a. In the Member of list, select the group from which to remove the user. Multiple groups may be selected by pressing **Ctrl** or **Shift** while clicking on the group names.

b. Click *Remove*. The groups will be moved to the Available Groups list.

4. Click *Save* and then click *Close*. The User Accounts window displays the changes.

NOTE: The DSView software obtains external group membership and external user information when a user logs in. If a user's group membership changes or the user is deleted externally, the DSView software will not see those changes until the next time that user logs in.

Changing the preemption level for a user

You may specify the preemption level for the user. See *Preemption Levels* on page 24 for more information.

To change the preemption level of a user:

1. In a User Accounts window, click on a username. *Name* will automatically be selected in the side navigation bar and the User Name window will open.
2. Click *Preemption Levels* in the side navigation bar. The User Preemption Level window will appear.
3. Select a preemption level (1-4) from the drop-down menu.
4. Click *Save* and then click *Close*. The User Accounts window will open including any changes.

Specifying user address information

NOTE: This property may only be modified for users using internal authentication. See *Managing Authentication Services* on page 58 for more information.

You may specify the home and business address for a user. Both names appear in the User Accounts window.

To specify address information for a user:

1. In a User Accounts window, click on a username. *Name* will automatically be selected in the side navigation bar and the User Name window will open.
2. Click *Addresses* in the side navigation bar. The User Address Properties window will appear.
3. Type the home address of the user.
4. Type the business address of the user.
5. Click *Save* and then click *Close*. The User Accounts window will open including any changes.

Specifying user phone contact information

NOTE: This property may only be modified for users using internal authentication. See *Managing Authentication Services* on page 58 for more information.

You may specify home, business, mobile and business mobile phone numbers and a pager number for a user. The numbers will appear in the User Accounts window. Assigning phone contact information may be helpful for quickly locating the person if an issue or question arises.

To specify phone contact information for a user:

1. In a User Accounts window, click on a username. *Name* will automatically be selected in the side navigation bar and the User Name window will open.
2. Click *Telephones* in the side navigation bar. The User Telephone Properties window will appear.
3. Type the home phone number, business phone number, mobile phone number, mobile business phone number and/or pager number of the user.
4. Click *Save* and then click *Close*. The User Accounts window will open including any changes.

Specifying email contact information for users

NOTE: This property may only be modified for users using internal authentication. See *Managing Authentication Services* on page 58 for more information.

You may specify a primary email address and up to five additional email addresses for a user. The email addresses will appear in the User Accounts window. Assigning email contact information may be helpful for notifying the person if an issue or question arises.

To specify email contact information for user:

1. In a User Accounts window, click on a username. *Name* will automatically be selected in the side navigation bar and the User Name window will open.
2. Click *E-Mail Addresses* in the side navigation bar. The User E-Mail Properties window will appear.
3. Type the primary email address of the user and up to five additional email addresses.
4. Click *Save* and then click *Close*. The User Accounts window will open including any changes.

Specifying user notes

NOTE: This property may only be modified for users using internal authentication. See *Managing Authentication Services* on page 58 for more information.

Notes contain future reference information about a user.

To specify notes about a user:

1. In a User Accounts window, click on a username. *Name* will automatically be selected in the side navigation bar and the User Name window will open.
2. Click *Notes* in the side navigation bar. The User Notes window will open.
3. Type the information you wish to note about the DSView user.
4. Click *Save* and then click *Close*. The User Accounts window will open including any changes.

Changing custom field properties

NOTE: This property may only be modified for users using internal authentication. See *Managing Authentication Services* on page 58 for more information.

Six custom fields for users are provided within the DSView management software. You may specify any information you wish in these fields for display in the User Accounts window.

To change the custom fields:

1. In a User Accounts window, click on a username. *Name* will automatically be selected in the side navigation bar and the User Name window will open.
2. Click *Custom Fields* in the side navigation bar. The User Custom Fields window will appear.
3. Type the information in the fields you wish to define.
4. Click *Save* and then click *Close*. The User Accounts window will open including any changes.

Displaying User Access Rights

The access rights of one or more user groups and/or users may be associated to one or more units. For example:

- A user is created with the login name johnsmith.
- The user is then assigned to the User Administrators group.
- A DSR1021 switch is added to the DSView software system.
- Using the Unit Access Rights window, the User Administrators group is assigned to the DSR1021 switch and various rights are assigned to the switch. The user johnsmith will have the rights assigned to the user administrators group as long as he is a member of the group. If johnsmith is removed from the user administrators group, he will no longer have the rights of the group.

  Alternatively, if the user administrators group was not going to be assigned access rights to the DSR1021 switch, access rights could be added for only the user johnsmith.

See *Adding User Accounts* on page 153, *Managing User Groups* on page 163 and *Changing Unit Access Rights* on page 102 for more information.

Customizing Appliance and Target Device Access Rights windows

By default, the Name field is always displayed in the target device Access Rights window. The following fields also display and may be removed by clicking the *Customize* link:

- Viewer Sessions - Specifies whether the user may display KVM sessions using a Video Viewer window or Serial sessions using a Telnet Viewer window.
- Power Control - Specifies whether the user may control the power of the target device if it is connected to an SPC device outlet.
- VM Sessions - Specifies whether the user may establish virtual media sessions.
- Reserved VM Sessions - Specifies whether the user may establish reserved virtual media sessions.

By default, the Name field is always displayed in the Appliance Access Rights window. The following fields also display and may be removed by clicking the *Customize* link:

- Reboot - Specifies whether the user may reboot the DS1800 digital switch, CPS appliance, CCM appliance or DSR switch. See *Rebooting* on page 251 for more information.
- Flash Upgrade - Specifies whether the user may Flash upgrade the DS1800 digital switch, CPS appliance, CCM appliance or DSR switch. See *To update the firmware of specific appliances of a specific type to DSView software compatibility* on page 465 for more information.
- Settings - Specifies whether the user may change the appliance settings of the DS1800 digital switch, CPS appliance, CCM appliance or DSR switch. See *Changing Managed Appliance Settings* on page 106 for more information.
- Local Users - Specifies whether the user may manage local accounts on the DS1800 digital switch, CPS appliance, CCM appliance or DSR switch. See *Changing local account settings* on page 127 for more information.

See *Using the Customize link in windows* on page 15 for more information.

.To display a user's access rights to a target device:

1. In a User Accounts window, click on a username. *Name* will automatically be selected in the side navigation bar and the User Name window will open.
2. Click *Access Rights* in the side navigation bar and then click *Target Devices*. The target device Access Rights window will open
   - Black check mark - the user has the right to perform the corresponding action.
   - Grey check mark - a group to which the user belongs has the right to perform the corresponding action.
   - No check mark - the indicated action may not be performed because access rights have not been specified on the target device for the user or group to which the user belongs.

   The access rights display may contain information that appears invalid. For example, virtual media access can be enabled to a target device that does not support it. Similarly, virtual media access could be enabled but KVM (Video Viewer) access may be disabled. See *About target device access rights* on page 104 for an explanation.

3. Click *Close* when you are finished reviewing the access rights. The User Accounts window will open.

To display a user's access rights to a managed appliance:

1. In a User Accounts window, click on a username. *Name* will automatically be selected in the side navigation bar and the User Name window will open.
2. Click *Access Rights* in the side navigation bar and then click *Appliances*. The Appliance Access Rights window will open:
   - Black check mark - the user has the right to perform the corresponding action.
   - Grey check mark - a group to which the user belongs has the right to perform the corresponding action.
   - No check mark - the indicated action may not be performed because access rights have not been specified on the managed appliance for the user or group to which the user belongs.
3. Click *Close* when you are finished reviewing the access rights. The User Accounts window will open.

Managing User Groups

Users that have been added to the DSView software system may be added to the following two types of user groups:

- Built-In - The DSView management software is delivered with six predefined user groups: Appliance Administrators, Auditors, DSView software administrators, Everyone, User Administrators and Users. All users are automatically included in the Everyone user group when they are added to the DSView software system. Users may be added to any of the other user groups. The privileges that a user has to perform tasks on the DSView software system is dependent on the built-in user group to which the user is a member. See *Built-in User Groups* on page 22 for more information.
- User-defined - You may also define your own custom groups, based on any criteria you wish. For example, you may want to define groups based on user administrators with read-only access, software developers at a specific location, global network infrastructure personnel based on job title and so on.

Built-in user groups appear in the User Groups - Built-in window and user-defined user groups appear in the User Groups - User Defined window. By default, the Preemption Level column will appear in the windows and display the preemption level of each user group. The views of the windows may be customized by clicking the *Customize* button to display the following columns:

- Authentication Server - Displays the authentication server assigned to the user. See *Managing Authentication Services* on page 58 for more information.
- Role - The role of a user-defined user group, which may be None, User, Auditor, Appliance Administrator, User Administrator or DSView software administrator. The role column for a built-in user group or a user-defined user group with a role of None will be empty.
- Type - The type of user group, which will be Built-in or User Defined.

See *Using the Customize link in windows* on page 15 for more information.

Group naming in external authentication services

Groups in Active Directory (AD) external authentication services are specified using a combination of their Active Directory folder and group name, minus the group container specified in the DSView software.

The group container defaults to the AD domain root if it is unspecified.

For example, if you have an AD external authentication service for the “sw.eng.mydomain.com” domain with no group container specified, The “Domain Users” group in the “sw.eng.mydomain.com/Users” folder will have a DSView software equivalent of “Users/Domain Users”.

Using the same example, but with a group container of “Users”, the DSView software equivalent is “Domain Users”.

Using the same example, but with a group container of “mydomain.com”, the DSView software equivalent is “eng/sw/Users/Domain Users”.

Groups in LDAP external authentication services are specified using a modified distinguishedName of their LDAP object, minus the group base DN specified in the DSView software.

For example, if you have an LDAP external authentication service with a group base DN of “ou=myldap,c=US”, the “cn=Admin Users,ou=Users,o=myldap,c=US” group will have a DSView software equivalent of “Admin Users”.

Using the same example, but with the “cn=Admin Users,c=Sunrise,ou=Users,o=myldap,c=US” group, the DSView software equivalent is “Sunrise/Admin Users”.

To display user groups:

1. Click *Users* in the tab bar.
2. Click *Groups* in the top navigation bar. *Built-In* will automatically be selected in the side navigation bar and the User Groups - Built-in window will open.

   -or-

   Click *User-Defined* in the side navigation bar. The User Groups - User Defined window will open.

Adding user-defined user groups

If you are using DSView Internal authorization, you may add your own custom user-defined user groups. Once a user-defined user group is created, you may add other users that use DSView internal authentication as members.

External user-defined user groups may be added, but their membership is not controlled by the DSView software.

To add a user-defined user group:

NOTE: You must have DSView software administrator or user administrator rights to add user-defined user groups.

1. Click *Users* in the tab bar. Click *Groups* in the top navigation bar. Click *User-Defined* in the side navigation bar.
2. In the User Groups - User Defined window, click *Add*. The Add User Group wizard will appear. Click *Next*.
3. The Select Authentication Service window will open. This window contains a list of the names of all authentication servers that may be used to authenticate the user group when the user logs in. See *Managing Authentication Services* on page 58 for more information.

   Click on the name of an authentication service and then click *Next*.

   If you selected *DSView Internal* as the authentication service, continue to step 4.

   If you selected any other type of authentication service, go to step 5.
4. The Type in Internal Group Name window will open. Type the name for the new user group you wish to create, and then click *Next*. User-defined user group names may contain up to 64 non-case sensitive characters. User-defined user group names are case-preserving.

   Continue to step 7.
5. The Specify External Group Name window will open.
   a. Click *Import Everyone* to consider any user on the external authentication server as a member of this user group.

      -or-

      Click *Specify a group on external authentication service* and type the name of the group in the field. User group names may contain up to 64 non-case sensitive characters. User group names are case-preserving if the user group on the external authentication server is case sensitive. See *Group naming in external authentication services* on page 164 for more information.

      -or-

      Click *Find a group on external authentication service* to browse a list of groups on the external authentication service.

   b. Click *Next*.

   If you selected *Find a group on external authentication service*, continue to step 6.

   -or-

   If you selected *Specify a group on external authentication service*, go to step 7.
6. The Select Group from External Authentication Service window displays. If the list of groups contains more than 5000 entries, a message will indicate that not all items are displayed.

Select a group from the list and then click *Next*. You may filter the list by using the Filter button and the adjacent text field. See *Filtering information in a window* on page 13 for more information.

7. The Select Role window will open. Select a role for the user group: None, User, Auditor, Appliance Administrator, User Administrator or DSView software administrator, then click *Next*. See *Built-in User Groups* on page 22 for information about user roles.
8. The Select User Group Preemption Level window will open. Type a preemption level (from 1-4), or select a value in the drop-down menu, and then click *Next*. See *Preemption Levels* on page 24 for more information.
9. The Completed Successful window will open. Click *Finish*. The user group has been added.

Deleting user-defined user groups

You may delete any user-defined user groups that have been created in the DSView software system.

NOTE: You must have DSView software administrator or user administrator rights to delete user-defined user groups.

To delete a user-defined user group:

1. Click *Users* in the tab bar. Click *Groups* in the top navigation bar. Click *User-Defined* in the side navigation bar.
2. In the User Groups - User Defined window, click the checkbox to the left of the user groups you wish to delete.

   -or-

   Click the checkbox to the left of Name at the top of the list to select all user groups listed in the window for deletion.
3. Click *Delete*. A confirmation dialog box will appear.
4. Click *Yes* to confirm or *No* to cancel.

Displaying and changing user group properties

To display the properties of a built-in user group:

1. Click *Users* in the tab bar. Click *Groups* in the top navigation bar. *Built-In* will automatically be selected in the side navigation bar and the User Groups - Built-in window will open.
2. Click on a user group name. The User Group Properties window will open. The display includes read-only properties for each group: name, type and preemption level.
3. Click *Close* when you are finished. The User Groups - Built-in window will open.

To display or change the properties of a user-defined user group:

1. Click *Users* in the tab bar. Click *Groups* in the top navigation bar. Click *User-Defined* in the side navigation bar. The User Groups - User Defined window will open.

2. Click on a user group name. The User Group Properties window will open. The side navigation bar includes the name of the user group at the top.
3. To change the name of the user group, type a new name in the Name field.

   To change the preemption level, type a number (from 1-4) in the Preemption Level field, or select a value in the drop-down menu. The higher the number, the higher the preemption level. See *Preemption Levels* on page 24 for more information.

   To change the role of the user group, select a role in the drop-down menu. If you do not wish to assign a role to the user group, select *None*.
4. Click *Save* and then click *Close*. The User Groups - User Defined window will open, including any changes.

Displaying and changing user group members

When users are created, they may be assigned to one or more built-in or user-defined user groups. You may add or remove users to or from the built-in and user-defined user groups.

To add or remove user group members:

NOTE: Members may only be assigned to or removed from user groups defined on the Internal DSView authentication server.

1. Click *Users* in the tab bar.
2. Click *Groups* in the top navigation bar. *Built-In* will automatically be selected in the side navigation bar and the User Groups - Built-in window will open.

   -or-

   Click *User-Defined* in the side navigation bar. The User Groups - User Defined window will open.
3. Click on a user group name. The User Group Properties window will open.
4. Click *Members* in the side navigation bar. The User Group Members window will open.
5. Click *Assign*. The Assign Users to User Group window will open.
6. To add a user to the user group:
   a. Select the user to add in the Available Users list. Multiple users may be selected by pressing **Ctrl** while clicking on the users.
   b. Click *Add*. The users will be moved to the Members list.

   -or-

   To remove a user from the user group:
   a. Select the user which you wish to remove in the Members list. Multiple users may be selected by pressing **Ctrl** while clicking on the users.
   b. Click *Remove*. The users will be moved to the Available Users list.
7. Click *Save* and then click *Close*. The User Group Members window will open, including any changes.

8. Click *Close*. The User Group - Built-In or User Group - User Defined window will open (depending on which groups you were working with).

NOTE: You may also add or remove a user from a built-in or user-defined user group by clicking on a username in a User Accounts window and changing its user group membership. See *Changing user group membership* on page 158 for more information.

Displaying user group unit access rights

Different built-in and user-defined user groups provide different access rights for units. Access rights determine which actions you may or may not perform on a unit. You may display the units that belong to a built-in or user-defined user group and the access rights provided to each by the built-in or user-defined user group.

Target devices appear in the Target Device Access Rights window, while managed appliances appear in the Appliance Access Rights window.

For information about assigning or changing unit access rights, see *Changing Unit Access Rights* on page 102.

Customizing the Unit Access Rights windows

By default, the following columns display in the Target Device Access Rights window and may be removed by clicking the *Customize* link:

- Viewer Sessions - Whether a user may open a DSView software session with a target device using a Video Viewer window.
- Power Control - Whether a target device connected to an SPC device outlet may be powered up, powered down or have its power cycled.
- VM Sessions - Whether a user may establish virtual media sessions.
- Reserved VM Sessions - Whether a user may establish reserved virtual media sessions.

By default, the following columns display in the Appliance Access Rights window and may be removed by clicking the *Customize* link:

- Reboot - Whether a user assigned to the built-in user group may reboot the managed appliance.
- Flash Upgrade - Whether a user assigned to the built-in user group may Flash upgrade the managed appliance.
- Settings - Whether a user assigned to the built-in user group may configure the settings of the managed appliance.
- Local Users - Whether a user assigned to the built-in user group may configure the local user account of a DS1800 digital switch, CPS appliance, CCM appliance or DSR switch.

See *Using the Customize link in windows* on page 15 for more information.

To display the access rights of a target device in a user group:

1. Click *Users* in the tab bar.

2. Click *Groups* in the top navigation bar. *Built-In* will automatically be selected in the side navigation bar and the User Groups - Built-in window will open.

   -or-

   Click *User-Defined* in the side navigation bar. The User Groups - User Defined window will open.
3. Click on a user group name. The User Group Properties window will open.
4. Click *Access Rights* in the side navigation bar. *Target Devices* will automatically be selected in the side navigation bar and the Target Devices Access Rights window will open.

   A check (√) will appear in the corresponding column if the access right is available for the unit. The column will be empty if the access right is not granted. See *Changing Unit Access Rights* on page 102 for more information.

   The access rights display may contain information that appears invalid. For example, virtual media access can be enabled to a target device that does not support it. Similarly, virtual media access could be enabled but KVM (Video Viewer) access may be disabled. See *About target device access rights* on page 104 for an explanation.
5. Click *Close* when you are finished. The User Accounts - All window will open.

To display the access rights of a managed appliance in a user group:

1. Click *Users* in the tab bar.
2. Click *Groups* in the top navigation bar. *Built-In* will automatically be selected in the side navigation bar and the User Groups - Built-in window will open.

   -or-

   Click *User-Defined* in the side navigation bar. The User Groups - User Defined window will open.
3. Click on a user group name. The User Group Properties window will open.
4. Click *Access Rights* in the side navigation bar, and then click *Appliances*. The Appliance Access Rights window will open.

   A check (√) will appear in the corresponding column if the access right is available for the unit. The column will be empty if the access

   right is not granted. See *Changing Unit Access Rights* on page 102 for more information.
5. Click *Close* when you are finished. The User Accounts - All window will open.

CHAPTER 6

Using the Video Viewer

The Video Viewer is used to conduct a KVM session with one or more target devices attached to one or more DS1800 digital switches or DSR switches. When you connect to a device using the Video Viewer, the target device desktop appears in a separate window. You will see both the local and the target device cursor. The Video Viewer window supports either a 3 or 5 button mouse.

Virtual media sessions, which are supported on some DSR switches, are opened from the Video Viewer.

About the Video Viewer Window

The DSView management software uses either a Java-based program or an ActiveX applet to display the Video Viewer window. The Java-based Video Viewer is launched from the Mozilla, Firefox and Netscape based clients when a KVM session is requested. The ActiveX Video Viewer is launched from Internet Explorer on Windows.

NOTE: The DSView management software uses system memory to store and display images within Video Viewer windows. Each opened Video Viewer window requires additional system memory. An 8-bit color setting on the Client PC requires 1.4 MB of memory per Video Viewer window, a 16-bit color setting requires 2.4 MB and a 32-bit color setting requires 6.8 MB. Opening more than four simultaneous Video Viewer windows may affect system performance and is not recommended. If you attempt to open more Video Viewer windows than your system memory allows, you will receive an out of memory error and the requested Video Viewer window will not open.

KVM sessions may be launched to devices from any DS1800 digital switch or DSR switch. Each KVM session will be established using the configured encryption level. See *Displaying and changing session settings on managed appliances* on page 121 for more information.

If the device you are attempting to access is currently being viewed by another user and you have administrator privileges, you may disconnect the other user so that you may access that device.

You cannot preempt a local user who is in Broadcast mode. See the DSR Installer/User Guide for more information.

Video Viewer minimum requirements

The Video Viewer requires one of the following operating systems:

- Windows 2000 Workstation or Server with Service Pack 2
- Windows Server 2003 Standard, Enterprise or Web Edition
- Window NT 4.0 Workstation or Server with Service Pack 6a
- Windows XP Home Edition or Professional
- Red Hat Enterprise Linux

The Video Viewer may use any of the browsers supported for the DSView Explorer; see *Web-based access and control* on page 1 for more information.

The Video Viewer client requires Java when launched from Mozilla, Netscape or Firefox browsers. The supported Java version is 1.5.0_02. The Video Viewer requires this version. The DSView software client automatically downloads and installs the JRE (Java Runtime Environment) the first time the Video Viewer or Telnet Viewer is launched. See *Java Installation* on page 47 for more information.

To launch a KVM session, a user must be individually assigned rights or belong to a user group which has been assigned rights to establish a KVM session. See *Changing Unit Access Rights* on page 102 for more information. You may review which users may establish KVM session connections at the user level. See *Displaying User Access Rights* on page 161 for more information.

Launching a KVM Session

NOTE: When using a non-proxied connection, video performance over a slower network connection may be less than optimal. Since certain color settings (such as grayscale) use less network bandwidth than others (such as Best Color), changing the color settings may increase video performance. For optimal video performance over a slower network connection, a color setting such as Grayscale/Best Compression or Low Color/High Compression is recommended. See *Adjusting color depth* on page 181 for more information.

To launch a KVM session from the DSView Explorer:

1. Display a Target Devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window. See *About Unit Views* on page 81 for more information.
2. Click the *KVM Session* link in the Action column of the target device you wish to view.

   The Video Viewer launches in a new window.

To launch a KVM session using the Unit Overview window:

1. Display a Target Devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window. See *About Unit Views* on page 81 for more information.
2. Click on the name of a target device connected to a DS1800 digital switch or DSR switch. The side navigation bar will contain the name of the target device at the top and *Overview* will automatically be selected. The Unit Overview window will open.

3. Click on the *KVM Session* name or icon.

   The Video Viewer launches in a new window.

Launching an exclusive KVM session

If a user needs to access a port while excluding all other users, an exclusive KVM connection is used. When a port is selected with the Exclusive KVM connection setting enabled, no other user in the system may switch to that port. If a user initiates a connection to a port currently accessed by a different user using an exclusive KVM connection, the new user will receive a message indicating the port's status and will not be connected to the port.

To launch an exclusive (non-shared) KVM session from the DSView Explorer:

1. Display a Target Devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window. See *About Unit Views* on page 81 for more information.
2. Click the alternate actions arrow in the Action column of the target device you wish to view. A list of actions will appear.
3. Click the *Exclusive KVM Session* link.

   The Video Viewer launches in a new window. A yellow dot will appear next to the icon of the target device in the Target Devices, Units in Site, Units in Custom Field, Topology and Recently Accessed Units windows to indicate that the target device is using an Exclusive KVM connection. Other users may not share the session.

To launch an exclusive (non-shared) KVM session in the Unit Overview window:

1. Display a Target Devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window. See *About Unit Views* on page 81 for more information.
2. Click on the name of the target device to which you wish to establish an exclusive connection. The name of the target device and a list of item links will appear in the side navigation bar, *Overview* will be automatically selected in the side navigation bar and the Unit Overview window will appear.
3. Click *Exclusive KVM Session*.
4. Click the *KVM Session* icon or link in the Unit Overview window.

   The Video Viewer launches in a new window. A yellow dot will appear next to the icon of the target device in the Target Devices, Units in Site, Units in Custom Field, Topology and Recently Accessed Units windows to indicate that the target device is using an Exclusive KVM connection. Other users may not share the session.

Connecting to an existing session

When you attempt to connect to a port already in use by another user, the Cannot connect to the server dialog box displays and states that the port is in use along with the name of the current user(s). At this point, you may request to share access to the port with the current user(s).

You may be presented with one or more of the following options in the Cannot connect to the server dialog box:

- Actively share a connection - When the dialog box contains a statement prompting you to share a connection to the server and you click *Share with the other user* and do not click Passive Share, an active connection will be established. When sharing access to a port actively, all users may monitor the port and take control if no other user is currently active.

  When you click *OK* on the Cannot connect to the server dialog box, the primary user that is currently active will receive a request to allow sharing unless *Allow shared connections automatically* has been enabled (see *Specifying Video Viewer Session Settings* on page 177 for more information). If the user confirms, then you will gain active access to the port.
- Passively share a connection - When you click *Share with the other user* and also click *Passive Share* in the dialog box, a passive connection will be established. When sharing access to a port passively, you may only display what occurs on the server without controlling the keyboard or mouse.

  When you click *OK* on the *Cannot connect to the server* dialog box, the primary user that is currently active will receive a request to allow sharing unless *Allow shared connections automatically* has been enabled (see *Specifying Video Viewer Session Settings* on page 177 for more information). If the user confirms, then you will gain passive access to the port.
- Preempt a user's connection (DSView software administrators and user administrators only) - When the dialog box prompts you to preempt the user's session and you click *Preempt the other user*, the user requesting access to the target device will be connected and the existing user(s) will lose their connection to the target device. The existing user(s) will be notified that the session has been preempted.
- Make a stealth connection (DSView software administrators and user administrators only) - When the dialog box contains a statement asking if you wish to connect using Stealth mode and if you click *Stealth mode*, a Video Viewer window session will be started but you will only be able to display what occurs on the server without controlling the keyboard or mouse. The user that is currently active will not receive notification that access is being shared and no request to authorize sharing will be made.

Up to 12 users may share a single port at one time. If a 13th user attempts to connect, an error message will inform the user that no sessions are available.

At any time, a user may select *View - List of Shared Users* in a Video Viewer window to display a list of users sharing their port or channel. Users in Stealth mode are excluded from this list.

Session time-out

A remote session may time-out if there has been no activity in a Session window for a specified time. The session time-out value is configured by your DSView software administrator at the DS1800 digital switch or DSR switch level using the Appliance Session Settings window. See *Changing Managed Appliance Settings* on page 106 for more information.

You may override this value within the DSView Explorer. If you specify a new time-out value, it will be used the next time the DSView management software is started. See *Connecting to an existing session* on page 173 for more information.

Window Features

Figure 6.1 shows the Video Viewer window areas, and descriptions follow in Table 6.1.

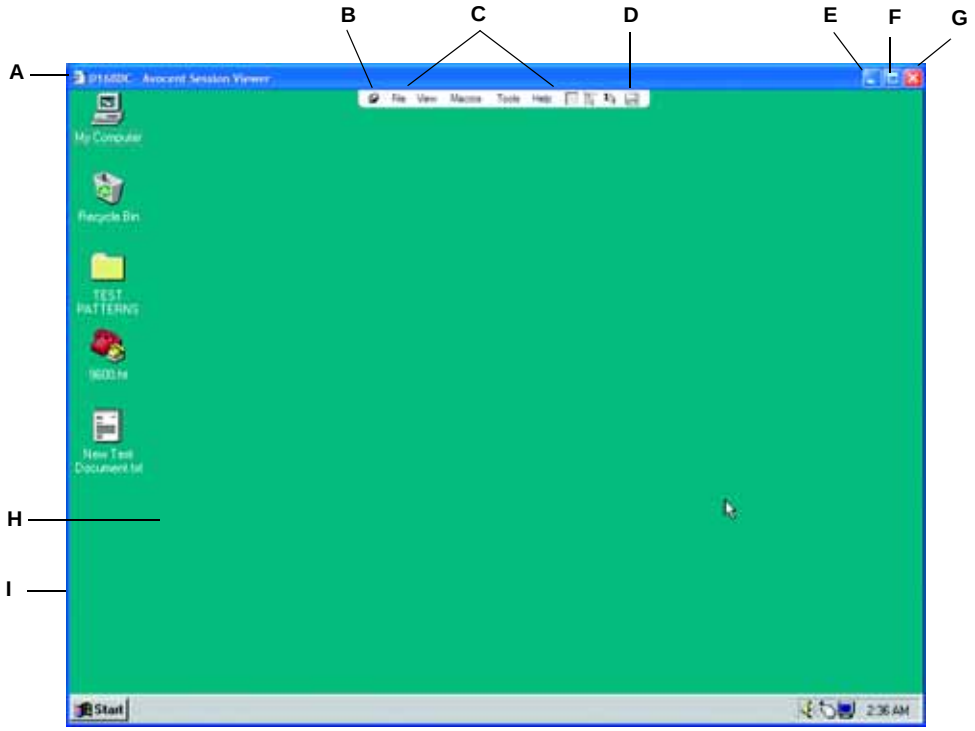


Figure 6.1: Video Viewer Window (Normal Window Mode)

Table 6.1: Video Viewer Window Descriptions

Letter	Description
A	Title Bar: Displays the name of the server being viewed. When in Full Screen mode, the title bar disappears and the server name appears between the menu and toolbar.
B	Thumbtack: Locks the display of the menu and toolbar so that it is visible at all times.
C	Menu and toolbar: Allows you to access many of the features in the Video Viewer window. The menu and toolbar will be in a show/hide state if the thumbtack has not been used. Place your cursor over the toolbar to display the menu and toolbar. Up to ten commands and/or macro group buttons may be displayed on the toolbar. By default, the Single Cursor Mode, Refresh, Automatic Video Adjust and Align Local Cursor buttons appear on the toolbar. See *Changing the toolbar* on page 177 and *Using Global and Personal Macros* on page 192 for more information.
D	Macro button: Displays when a user specifies icons for macros and indicates that the icons should appear on the toolbar. See *Using Global and Personal Macros* on page 192 for more information.
E	Minimize button: Minimizes the display of the Video Viewer window into the task bar at the bottom of the local computer.
F	Maximize button: Changes the window to Full Screen mode, which expands the accessed device desktop to fill the entire screen. When you expand the window, the following occurs: • The title bar disappears. • The server name appears between the menu and toolbar. • The Maximize button is changed to a Normal Window Mode button and it appears on the toolbar. Clicking the button will toggle the Video Viewer window to Normal Window mode. • The Close button appears on the toolbar.
G	Close button: Closes the VIdeo Viewer window.
H	Accessed device desktop: Interacts with your device through this window.
I	Frame: Resizes the Video Viewer window by clicking and holding on the frame.

NOTE: The Close button may not be present on all operating systems.

See the DSR Installer/User Guide for information about how the keys on a standard Type 5 Sun keyboard are emulated on a PS/2 keyboard.

Specifying Video Viewer Session Settings

To specify Video Viewer session settings:

NOTE: You must have DSView software administrator or user administrator privileges to specify Video Viewer session settings.

1. Click the *System* tab.
2. Click *Global Properties* in the top navigation bar. *Video Session Properties* will automatically be selected in the side navigation bar and the Video Viewer Session Properties window will open.
   a. Select *Allow shared connections automatically* if you wish to allow other users to share a Video Viewer session automatically. You will not be notified that they wish to connect to the session and will not be able to accept or reject the connection.

      -or-

      Leave the checkbox empty if you wish to be notified that other users wish to share the Video Viewer session. When a user attempts to connect to the session, you will be notified and allowed to either accept or reject their connection request.

   b. Select *View identity of shared connections* if you wish to display a list of shared connections using the *View - Connected Users* command. See *Displaying Video Viewer Users* on page 199 for more information.
3. Click *Save* and then click *Close*.

Changing the toolbar

You may choose the amount of time before the toolbar hides in the Video Viewer window when it is in show/hide state (that is, not locked in place by the thumbtack) and which commands and macros appear on the toolbar. See *Using Global and Personal Macros* on page 192 for more information.

To specify a toolbar hide time:

1. Select *Tools - Session Options* from the Video Viewer window menu.

   -or-

   Click the *Session Options* button.

   The Session Options dialog box appears.
2. Click the *Toolbar* tab.
3. Use the arrow keys to specify the number of seconds to delay the hiding of the toolbar.
4. Click *OK* to save your changes and close the dialog box.

To add or remove macros or commands from the toolbar:

1. Select *Tools - Session Options* from the Video Viewer window menu.

   -or-

   Click the *Session Options* button.

   The Session Options dialog box appears.
2. Click the *Toolbar* tab.
3. Select or deselect the checkboxes of the commands and macros you wish to display or remove from the toolbar.
4. Click *OK* to save your changes and close the dialog box.

Toggling menu and toolbar activation

You may specify a key that will show the menu and toolbar when they are hidden.

To select a key for toggling activation of the menu and toolbar:

1. Select *Tools - Session Options* from the Video Viewer window menu.

   -or-

   Click the *Session Options* button.

   The Session Options dialog box appears.
2. Click the *General* tab.
3. Select a keystroke from the drop-down menu in the Menu Activation Keystroke area.
4. Click *OK*. When you disable the menu and toolbar, the specified key may be pressed to reenable the menu and toolbar.

Setting the Window Size

NOTE: The View - Scaling command is not available if the Video Viewer window is in Full Screen mode or to non-primary users of a shared session.

When the DSView management software is used for the first time, any Video Viewer windows that are opened from a DS1800 digital switch or DSR switch port or channel in any DSView management software sessions will display at a resolution of 1024 x 768 until the value is changed by a user. Each Video Viewer window may be set to a different resolution.

The DSView management software will automatically adjust the display if the window size changes during a session as long as autoscaling is enabled. When a user accesses a channel using sharing, the display will be adjusted to match the input resolution selected by the primary user of that channel. This will prevent the primary user's display from being affected. If the target device resolution changes any time during a session, the display will be adjusted automatically.

To change the Video Viewer window resolution:

Select the *View - Scaling* command and then click on the desired resolution.

Adjusting the View

Using menus or Task buttons in the Video Viewer window, you may:

- Align the mouse cursors.
- Refresh the screen.
- Enable or disable Full Screen mode. When Full Screen mode is enabled, the image will be adjusted to fit the desktop up to a size of 1024 x 768. If the desktop has a higher resolution, the following will occur:
  - The full screen image will be centered in the desktop and the areas surrounding the Video Viewer window will be black.
  - The menu and toolbar will be locked so that they are visible at all times.
- Enable automatic, full or manual scaling of the session image. With automatic scaling, the desktop window remains fixed and the device image is scaled to fit the window. With full scaling, the desktop window is sized to match the resolution of the server being viewed. With manual scaling, a drop-down menu of supported image scaling resolutions is displayed.
- Change the color depth of the session image.

To align the mouse cursors:

Click the *Align Local Cursor* button in the Video Viewer window toolbar. The local cursor will align with the cursor on the remote device.

If cursors drift out of alignment, turn off mouse acceleration in the device.

To refresh the screen:

Click the *Refresh Image* button in the Video Viewer window.

-or-

Select *View* - *Refresh* from the Video Viewer window menu. The digitized video image will be completely regenerated.

NOTE: You may also specify background refreshing of the Video Viewer window by a DS1800 digital switch or DSR switch. See *Using background refresh* on page 180 for more information.

To enable or disable full screen mode:

NOTE: The View - Full Screen command may only be used by the primary user. The command is not available to non-primary users who are sharing the session.

1. To enable Full Screen mode, click the *Maximize* button.

   -or-

   Select *View* - *Full Screen* from the Video Viewer window menu.

The desktop window will disappear and only the accessed device desktop will be visible. The screen will be resized up to a maximum of 1024 x 768. If the desktop has a higher resolution, then a black background will surround the full screen image. The floating toolbar will appear.

2. To disable Full Screen mode, click the *Full Screen Mode* button on the floating toolbar to return to the desktop window.

To enable automatic, full or manual scaling:

NOTE: The View - Scaling command is not available if the Video Viewer window is in Full Screen mode or to non-primary users of a shared session.

To enable automatic scaling, select *View - Scaling* from the Video Viewer window menu. The device image will be scaled automatically.

-or-

To enable full scaling, select *View - Scaling* from the Video Viewer window menu. The device image will be scaled to the resolution of the server being viewed automatically.

-or-

To enable manual scaling, select *View - Scaling* from the Video Viewer window menu, then choose the dimension to scale the window. Available manual scaling sizes are:

1024 x 768	768 x 576
960 x 720	704 x 528
896 x 672	640 x 480
832 x 624	

Using background refresh

In addition to using the Refresh Image command, you may also choose to allow the DS1800 digital switch or DSR switch to background refresh the Video Viewer window. When this option is enabled, a small portion of video data is constantly sent by the DS1800 digital switch or DSR switch. When background refresh is not enabled, the Video Viewer window is updated by the DS1800 digital switch or DSR switch only when it determines that the target device video image has changed.

NOTE: This option is not available if the DS1800 digital switch or DSR switch being used to display the target device does not support background refresh or if the DSR Remote Operations software is being used to connect to the DSR switch viewing the target device. See *DSR Remote Operations Software* on page 301 for more information.

To enable or disable background refresh:

1. Select *Tools - Session Options* from the Video Viewer window menu.

   -or-

   Click the *Session Options* button.

   The Session Options dialog box appears.
2. Click the *General* tab.
3. Select *Background Refresh* to enable the option.

   -or-

   Uncheck *Background Refresh* to disable the option.
4. Click *OK*.

Adjusting color depth

NOTE: The View - Color command may only be used by the primary user. The command is not available to non-primary users who are sharing the session.

The DS1800 digital switch or DSR switch Dambrackas Video Compression™ (DVC) algorithm enables DSView management software users to adjust the number of viewable colors in a remote session window. You may choose to display more colors for the best fidelity, or fewer colors to reduce the volume of data transferred on the network.

The DVC algorithm upgrade is standard on all DS1800 digital switches and DSR switches supported by the DSView software.

Video Viewer windows can be viewed using the Best Color Available (slower updates), Best Compression (fastest updates), a combination of Best Color and Best Compression or in Grayscale.

The color depths of individual ports and channels can be specified by selecting the *View - Color* command in a remote session window. These settings are saved individually per port and channel.

Additional Video Adjustment

Generally, the Video Viewer window automatic adjustment features will optimize the video for the best possible view. However, users may fine tune the video with the help of Avocent Technical Support by using the *Tools - Manual Video Adjust* command in the Video Viewer window menu or clicking the *Manual Video Adjust* button. This displays the Manual Video Adjust dialog box.

Video adjustment is a per target setting and applies to each target device you access.

Modified video settings are written to the DS1800 digital switch or DSR switch. Settings are also stored per port/channel session on a system when they are made and saved so they may be used during a non-shared session as follows:

- If sharing is not enabled, the video settings made on the local DS1800 digital switch or DSR switch during the session are used.

- If sharing is enabled for the non-primary user, video settings are read from the DS1800 digital switch or DSR switch.

See *Connecting to an existing session* on page 173 for information about session sharing.

Users may verify the level of packets per second required to support a static screen by observing the packet rate which is located in the lower left-hand corner of the dialog box.

To manually adjust the video quality of the window:

NOTE: The following video adjustments should be made only on the advice and with the help of Avocent Technical Support.

1. Select *Tools - Manual Video Adjust* from the Video Viewer window menu.

   -or-

   Click the *Manual Video Adjust* button.

   The Manual Video Adjust dialog box appears. Figure 6.2 shows the dialog box; descriptions follow.
2. Click the icon corresponding to the feature you wish to adjust.
3. Move the slider bar and then fine tune the setting by clicking the *Min* (-) or *Max* (+) buttons to adjust the parameter for each icon pressed. The adjustments will display immediately in the Video Viewer window.
4. When finished, click *Close* to exit the Manual Video Adjust dialog box.

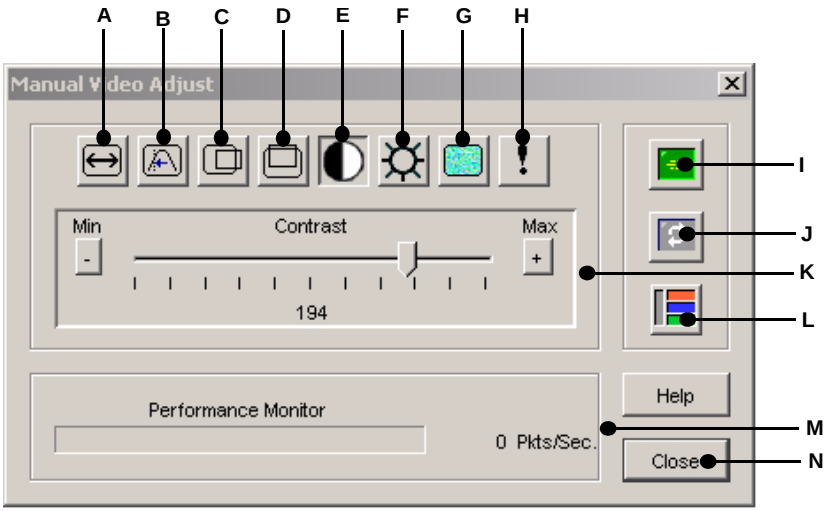


Figure 6.2: Manual Video Adjust Dialog Box

Table 6.2: Manual Video Adjust Dialog Box Descriptions

Letter	Description	Letter	Description
A	Image Capture Width	**H**	Pixel Noise Threshold
B	Pixel Sampling/Fine Adjust	**I**	Automatic Video Adjustment
C	Image Capture Horizontal Position	**J**	Refresh Image
D	Image Capture Vertical Position	**K**	Adjustment bar
E	Contrast	**L**	Video Test Pattern
F	Brightness	**M**	Performance Monitor
G	Block Noise Threshold	**N**	Close button

Image capture width, pixel sampling/fine adjust, image capture horizontal position and image capture vertical position

The Image Capture Width, Pixel Sampling/Fine Adjust, Image Capture Horizontal Position and Image Capture Vertical Position adjustments affect how the target video is captured and digitized and are seldom changed.

The image capture parameters are automatically changed by the Automatic Adjustment function. A special image is required on the target in order to make accurate adjustments independently.

Contrast and brightness

If the image in the Video Viewer window is too dark or too light, select *Tools - Automatic Video Adjust* or click the *Automatic Video Adjust button.* This command is also available in the Video Adjustments dialog box. In most cases, this will correct video problems. In those cases where clicking on Auto Adjust several times does not set the contrast and brightness as desired, adjusting the contrast and brightness manually may help.

First, increase the brightness. Do not go more than 10 increments before moving the contrast. Generally, the contrast should be moved very little.

Detection thresholds

In some cases, noise in the video transmission keeps the packets/sec count up. This may be seen when little dots change in the area of the cursor when it is moved. Varying the threshold values may result in “quieter” screens and improved cursor tracking.

Noise Threshold and Priority Threshold values may be modified if you are using standard video compression. Block Noise Threshold and Pixel Noise Threshold values may be modified if you are using the DS1800 digital switch or DSR switch DVC algorithm upgrade. Default threshold values can be restored by clicking *Auto Adjust Video*.

Block noise threshold and pixel noise threshold

The Block Noise Threshold and Pixel Noise Threshold values set the minimum color levels in terms of changed video blocks and pixels per thousand that are allowed.

- The Block Noise Threshold sets the minimum color change that will occur in a single video block. Increasing the value will reduce the network bandwidth. Decreasing the value will make the size of these artifacts smaller.
- The Pixel Noise Threshold sets the minimum color change in a single pixel. Decreasing the value will reduce the number of low-contrast artifacts, but will increase network bandwidth.

See *Adjusting the View* on page 179 for information about changing the color depth.

Automatic video adjustment

NOTE: You may also select *Tools - Automatic Video Adjust* from the Video Viewer window menu or click the *Automatic Video Adjust* toolbar icon to automatically adjust the video.

In most cases, you will not need to alter the Video Settings from the default. The system will automatically adjust and use the optimal video parameters. The DSView management software performs best when the video parameters are set such that no (0) video packets are transmitted for a static screen.

You may easily adjust your video parameters by clicking on the *Auto Adjust Video* button in the Manual Video Adjust dialog box, which instructs the DS1800 digital switch or DSR switch to optimize the video to ideal settings.

NOTE: A green screen with yellow lettering may appear during auto-adjustment.

Refresh image

NOTE: You may also select *View - Refresh* from the Video Viewer window menu to refresh the image.

Clicking the *Refresh Image* button in the Manual Video Adjust dialog box will completely regenerate the digitized video image.

Video test pattern

Clicking the *Video Test Pattern* button in the Manual Video Adjust dialog box will toggle a display of a video test pattern. Click the *Video Test Pattern* button again to toggle back to a normal video image.

Adjusting Mouse Options

The Video Viewer window mouse options affect cursor type, cursor mode, scaling, alignment and resetting. Mouse settings are device-specific; that is, they may be set differently for each device.

NOTE: If the device does not support the ability to disconnect and reconnect the mouse (almost all newer PCs do), then the mouse will become disabled and the device will have to be rebooted.

Cursor Type

The Video Viewer window offers five appearance choices for the local mouse cursor. You may also choose no cursor or the default cursor.

Single cursor mode

NOTE: Single cursor mode is available only on supported Windows system clients.

In Single Cursor mode, the display of the local (second) cursor in the Video Viewer window is turned off and only the target device mouse pointer will be visible. The only mouse movements that will appear are those of the target device remote cursor. Single Cursor mode is used when there is no need for a local cursor.

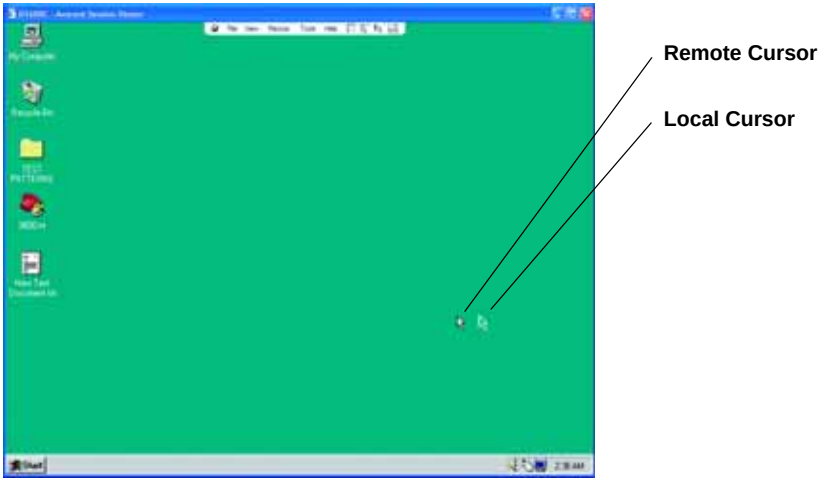


Figure 6.3: Video Viewer Window with Local and Remote Cursors Displayed

The cursor mode status of the Video Viewer window displays in the title bar, including the keystroke that will exit Single Cursor mode. You may define the keystroke that will exit Single Cursor mode in the Session Options dialog box.

NOTE: When using a device that captures keystrokes before they reach the client, you should avoid using those keys to restore the mouse pointer.

To enter single cursor mode:

Select *Tools - Single Cursor Mode* from the Video Viewer window menu. The local cursor will not appear and all movements will be relative to the target device.

-or-

Click the *Single Cursor Mode* button.

To select a key for exiting single cursor mode:

1. Select *Tools - Session Options* from the Video Viewer window menu.

   -or-

   Click the *Session Options* button.

   The Session Options dialog box appears.
2. Click the *Mouse* tab.
3. Select a terminating keystroke from the drop-down menu in the Single Cursor mode area.
4. Click *OK*. When you enable Single Cursor mode, the specified key may be pressed to return to Regular Desktop mode.

To exit single cursor mode:

Press the key on the keyboard that is identified in the title bar.

Cursor settings

When using the DSView software, your mouse pointer will change shape when over a Video Viewer window. You may change the appearance of this second local cursor or eliminate it.

To change the mouse cursor setting:

1. Select *Tools - Session Options* from the Video Viewer window menu.

   -or-

   Click the *Session Options* button.

   The Session Options dialog box appears.
2. Click the *Mouse* tab.
3. Select a mouse cursor type in the Local Cursor panel.
4. Click *OK*.

Scaling

You may choose among three preconfigured mouse scaling options or set your own custom scaling. The preconfigured settings are: Default (1:1), High (2:1) or Low (1:2), as follows:

- In a 1:1 scaling ratio, every mouse movement on the desktop window will send an equivalent mouse movement to the server.
- In a 2:1 scaling ratio, the same mouse movement will send a 2X mouse movement.

- In a 1:2 scaling ratio, the value will be 1/2X.

To set mouse scaling:

1. Select *Tools - Session Options* from the Video Viewer window menu.

   -or-

   Click the *Session Options* button.

   The Session Options dialog box appears.
2. Click the *Mouse* tab.
3. To use one of the preconfigured settings, check the appropriate radio button.
4. To set custom scaling, click the *Custom* radio button. The X and Y fields become enabled. Type a mouse scaling value in the X and Y fields. For every mouse input, the mouse movements are multiplied by the respective X and Y scaling factors. Valid input ranges are 0.25-3.00.

Alignment

Because the DSView management software cannot get constant feedback from the mouse, there are times when the mouse on the DS1800 digital switch or DSR switch may lose sync with the mouse on the host system. If your mouse or keyboard no longer responds properly, you may align the mouse to re-establish proper tracking.

Alignment causes the local cursor to be aligned with the cursor on the remote server. Resetting causes the appliance to simulate a mouse and keyboard reconnect at the device as if you had disconnected and then reconnected them.

To realign the mouse:

Click the *Align Local Cursor* button in the Video Viewer window toolbar.

Using Scan Mode

NOTE: Scan mode is not available when using the Topology Unit View window.

When the checkboxes of two or more target devices are selected in the DSView Explorer, the Scan button will become available. If the *Scan* button is clicked, Scan mode will be started and the Video Viewer windows will appear in the Thumbnail Viewer. A series of thumbnail frames appear in the Thumbnail Viewer, each containing a small, scaled, non-interactive version of a target device screen image.

The Scan mode moves from one thumbnail image to the next, logging into a device and displaying an updated device image for a specified length of time (View Time Per Server), before logging out of that device and moving on to the next thumbnail image. You may also specify a scan delay between thumbnails (Time Between Servers). During the delay, you will see the last thumbnail image for all devices in the scan sequence, though you won’t be logged into any devices.

When you first launch the Thumbnail Viewer, each frame will be filled with a white background until a device image is displayed. An indicator light at the bottom of each frame displays the device status. The default thumbnail size is based on the number of devices in the scan list.

Scan mode has a lower priority than an active connection. If you or another user are connected to a device, that device will be skipped in the scan sequence, and Scan mode will proceed to the next device unless the Shared Connections Automatically option has been selected, in which case target devices may be shared and will not be skipped in the scan sequence. No login error messages will appear. After your interactive session is closed, the thumbnail will be included in the scan sequence again.

You may disable a device thumbnail from the scan sequence. The thumbnail image remains, but it is not updated until it is once again enabled.

When running Scan mode, it is recommended that logging of the following events (enabled by default) are disabled in the DSView software system:

- Appliance Change Of State
- Appliance Viewer Session Started
- Appliance Viewer Session Stopped
- Viewer Session Started
- Viewer Session Stopped

Each thumbnail scan will result in the logging of the above events. The event log could grow to a huge size if the events are enabled and Scan mode is left running continuously for a length amount of time.

Thumbnail Viewer features

Figure 6.4 shows the Thumbnail Viewer areas, and descriptions follow in Table 6.3.

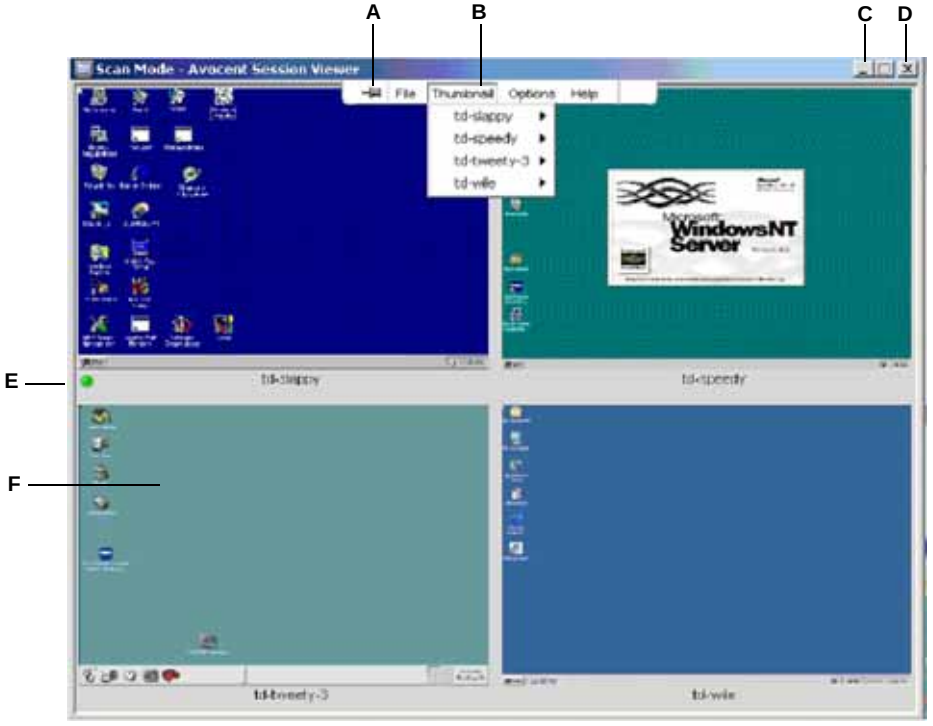


Figure 6.4: Thumbnail Viewer

Table 6.3: Thumbnail Viewer Descriptions

Letter	Description
A	Thumbtack: Locks the display of the menu so that it is visible at all times.
B	Menu: Allows access to Thumbnail Viewer features. The menu will be in a show/hide state if the thumbtack has not been used. Place your cursor over the toolbar to display the menu.
C	Minimize button: Minimizes the display of the Thumbnail Viewer window into the toolbar at the bottom of the local computer.
D	Close button: Closes the Thumbnail Viewer and all thumbnails being viewed.
E	Status indicator: The device name and status indicator appear below each thumbnail: • A green LED indicates that a device is currently being scanned. • A red X indicates that the last scan of the device was not successful. The scan may have failed due to a credential or path failure (for example, the device path on the appliance was not available). The tool tip for the LED indicates the reason for the failure.
F	Thumbnail image: Interacts with your device through this window.

NOTE: The Close button may not be present on all operating systems.

Performing Thumbnail Viewer tasks

To set scan preferences:

1. Select *Options* - *Preferences* from the Thumbnail Viewer menu. The Scan Mode Preferences dialog box appears.
2. In the View Time Per Server field, enter the time each thumbnail will be active during the scan, in the range 10-60 seconds.
3. In the Time Between Server field, enter the time the scan will stop between each device, in the range 5-60 seconds.
4. Click *OK*.

To pause or restart a scan sequence:

Select *Options* - *Pause Scan* from the Thumbnail Viewer menu. The scan sequence will pause at the current thumbnail if the Thumbnail Viewer has a scan in progress or will restart the scan if currently paused.

To change the thumbnail size:

Select *Options* - *Thumbnail Size* from the Thumbnail Viewer menu. Choose the desired thumbnail size from the cascade menu.

To disable a device thumbnail in the scan sequence:

Select a device thumbnail. Select *Thumbnail* - <*device name*> - *Disable* from the Thumbnail Viewer menu.

-or-

Right-click on a device thumbnail and select *Disable* from the pop-up menu. Updating of the thumbnail image will stop until it is enabled.

To enable a device thumbnail in the scan sequence:

Select a device thumbnail. Select *Thumbnail* - <*device name*> - *Enable* from the Thumbnail Viewer menu.

-or-

Right-click on a device thumbnail and select *Enable* from the pop-up menu.

Updating of that thumbnail image will resume.

To launch a session to a device from the Thumbnail Viewer:

Select a device thumbnail. Select *Thumbnail* - <*device name*> - *View Interactive Session* from the Thumbnail Viewer menu.

-or-

Right-click on a device thumbnail and select *View Interactive Session* from the Thumbnail Viewer menu. That target device desktop will appear in a Video Viewer window.

-or-

Double-click on the thumbnail image.

To exit the Thumbnail Viewer:

Select *File - Exit*.

-or-

Click the *Close* button.

Using Keyboard Pass-through

Keystrokes that a user enters when using a Video Viewer window may be interpreted in two ways, depending on the screen mode of the Video Viewer window.

If a Video Viewer window is using Full Screen mode, all keystrokes and keyboard combinations except **Ctrl-Alt-Del** are sent to the remote server being viewed. If a Video Viewer window is using Regular Desktop mode, Keyboard Pass-through mode may be used to control whether the remote server or local computer will recognize certain keystrokes or keystroke combinations.

Keyboard pass-through must be specified using the Session Options dialog box. When enabled, keyboard pass-through will send all keystrokes and keystroke combinations except **Ctrl-Alt-Del** to the remote server being viewed when the Video Viewer window is active. When the local desktop is active, keystrokes and keystroke combinations entered by the user affect the local computer.

NOTE: The **Ctrl-Alt-Delete** keyboard combination can only be sent to a remote server by using a macro. See *Using Global and Personal Macros* on page 192 for more information.

NOTE: The Japanese keyboard **ALT-Han/Zen** keystroke combination is always sent to a remote server, regardless of the screen mode or keyboard pass-through setting.

To specify keyboard pass-through:

1. Select *Tools - Session Options* from the Video Viewer window menu.

   -or-

   Click the *Session Options* button.

   The Session Options dialog box appears.
2. Click the *General* tab.
3. Select *Pass-through all keystrokes in regular window mode*.
4. Click *OK*.

Using Global and Personal Macros

NOTE: Macros may not be created, edited, copied or deleted if the DSR Remote Operations software is being used to connect to the DSR appliance viewing the target device. See *DSR Remote Operations Software* on page 301 for more information.

NOTE: You must have Appliance Administrator privileges to create and change Global Macros. See *Built-in User Groups* on page 22 for more information.

Three types of macros are available in the DSView management software. Exit macros are created within the DSView Explorer and are used by and located on DS1800 digital switches and DSR switches. See *Defining exit macros* on page 125 for more information.

The other two types, global macros and personal macros, are created and used by the Video Viewer. Global macros are created and maintained by users with administrative privileges and are stored on the hub server and any specified spoke servers. See *Displaying and changing session settings on managed appliances* on page 121 for more information.

NOTE: Global and personal macros may also be created in the Telnet Viewer window. Macros created using the Telnet Viewer window are not compatible with the Video Viewer and may only be used with target devices connected to CPS or CCM appliances.

Users may create personal macros for their own use. These macros can be accessed on the local computer using the Video Viewer window. Personal macros may be customized and grouped in any manner you wish with the exception of being included in a Global Macro group.

When a session is started in the DSView management software, global and personal macros are retrieved from the DSView software server. Then, when a Video Viewer window session is started, the macros are loaded. A user may choose to use either personal macros or global macros and switch between using them at any time during the session.

Both personal and global macros may be added to the Video Viewer window toolbar by assigning an icon to them using the Toolbar tab on the Session Options dialog box. A user may then execute the macro by clicking the button on the toolbar. See *Changing the toolbar* on page 177 for more information.

The Video Viewer window macro function allows you to:

- Send multiple keystrokes to a device, including keystrokes that you cannot generate without affecting your local system, such as **Ctrl-Alt-Delete**.
- Send a macro from a predefined macro group. Macro groups for Windows, Novell and Sun are already defined.
- Create, edit and delete your own macros. When you create or edit a macro, you may type the desired keystrokes or you may select from among several available categories of keystrokes. Each category contains a set of keystroke combinations. Selecting from the available categories and keystrokes saves time and eliminates the risk of typographical errors.

Since the DSView management software may be used to access different computer platforms, users may find it helpful to assign distinct macro groups to Global Macros or Personal Macros on

individual systems. You may group macros by selecting the *Macros - Configure - Macro Groups* command in the Video Viewer window and specifying the macro group to display in the Macro Groups dialog box.

The Macro Groups dialog box may also be used to switch between using Global and Personal Macros at any time during a session.

The Video Viewer window contains grouping commands that allow you to:

- Create, edit and delete your own macro groups. A user with software administrator or user administrator privileges may also change the predefined macro groups.
- Change the macro group that displays by default. This causes the macros in the specified group to be available on the Macros menu.

Macro group settings are device-specific; that is, they may be set differently for each device.

NOTE: Exit Macros, which reside on and are used by a DS1800 digital switch or DSR switch, may also be created. See *Defining exit macros* on page 125 for more information.

To send a macro:

1. Select *Macros* - <*desired macro*> from the Video Viewer window menu.

   -or-

   Select *Macros* - *Configure* - *Macros* from the Video Viewer window menu.

NOTE: The Macros - Configure - Macros menu item is not available if you are using the DSR Remote Operations software.

   -or-

   Click the *Macros* button.

   The Macros dialog box appears.
2. Select one of the following:

   All - displays both personal and global macros.

   Personal - displays personal macros only.

   Global - displays global macros only.
3. Select the desired macro from the Defined Macros list and then click *Run*.
4. Click *Close* when you are finished.

To create or edit a macro:

NOTE: Macros cannot be created or edited if you are using the DSR Remote Operations software.

1. Select *Macros* - *Configure* - *Macros* from the Video Viewer window menu.

   -or-

   Click the *Macros* button.

   The Macros dialog box appears.

2. To create a macro, click *Create*.

   -or-

   To edit a macro, click *Edit*.

   The Create Macro or Edit Macro dialog box appears.
3. If you are creating a macro, type a 1-32 character name in the Macro Name field.
4. Select whether you wish to edit or create a personal or global macro from the Macro Type area.
5. Select the type of keyboard you wish to use to create or edit the macro from the Keyboard Type drop-down menu. Available keyboard types are: U.S. English, Dutch, Danish, German, French, Italian, Spanish and Japanese.

   Select an icon to associate with the macro from the Macro Icon drop-down menu.
6. To build the macro, click on the keys on the virtual keyboard in the dialog box that you wish to use to create the macro. The keys of the virtual keyboard operate like a physical keyboard. As a key is clicked, it will appear in the Keystrokes list box to the left of the virtual keyboard.

   You may type or press the arrow keys to specify a delay between keys. First, click the key in the list box after which you wish to place a delay. Next, click *Delay* to insert the delay in the list box.

   Keystrokes unique to Sun keyboards may be added to the macro by selecting the key type from the drop-down menu to the right of the Sun Key button and clicking the button.
7. If necessary, use the following keys to change the entries in the Keystrokes list box:
   - Click *Reset* to remove all entries from the list box.
   - Click on an entry and then click *Remove* to remove it from the list box.
   - Click on an entry and then click *Move Up* to promote the entry in the list box.
   - Click on an entry and then click *Move Down* to demote the entry in the list box.
8. Click *OK* to accept the changes and return to the Macros dialog box.

   -or-

   Click *Cancel* to exit the Macros dialog box without saving your changes.

To delete a macro:

NOTE: Macros cannot be deleted if you are using the DSR Remote Operations software.

1. Select *Macros* - *Configure* - *Macros* from the Video Viewer window menu.

   -or-

   Click the *Macros* button.

   The Macros dialog box appears.
2. Select one of the following:

   All - displays both personal and global macros.

   Personal - displays personal macros only.

Global - displays global macros only.

3. Select the desired macro from the Defined Macros list and then click *Delete*. You are prompted to confirm the deletion.
4. Click *Yes* to confirm or *No* to cancel.
5. Click *Close* to exit the Macros dialog box.

To copy a macro:

NOTE: Macros cannot be copied if you are using the DSR Remote Operations software.

1. Select *Macros* - *Configure* - *Macros* from the Video Viewer window menu.

   -or-

   Click the *Macros* button.

   The Macros dialog box appears.
2. Select one of the following:

   All - displays both personal and global macros.

   Personal - displays personal macros only.

   Global - displays global macros only.
3. Select the desired macro from the Defined Macros list and then click *Copy.* The Copy Macro dialog box will appear.
4. Type a 1-32 character name in the Name of copied macro field.
5. Select whether you wish to make the copied macro a personal or global macro from the Macro Type area.
6. Click *OK* to copy the macro. The Copy Macro dialog box is closed and the copied macro will appear in the Macros dialog box.

   -or-

   Click *Cancel* to cancel the action.
7. Click *Close* to exit the Macros dialog box.

To create a macro group:

NOTE: Macro groups cannot be created if you are using the DSR Remote Operations software.

1. Select *Macros* - *Configure* - *Macro Groups* from the Video Viewer window menu.

   -or-

   Click the *Macro Groups* button.

   The Macro Groups dialog box appears.
2. Click *Create*. The Create/Edit Macro Group dialog box will appear.
3. In the Macro Group Name field, enter a 1-32 character unique macro group name.
4. In the Group Type area, click *Global* if you wish to create a Global Macro group.

-or-

Click *Personal* if you wish to create a personal macro group.

5. Click *OK* to save the name and return to the Macro Groups dialog box.

   -or-

   Click *Cancel* to leave the dialog box without saving changes.

6. Click *Close* to exit the Macro Groups dialog box.

To add or delete macros in an existing macro group:

NOTE: Macros cannot be added to or deleted from macro groups if you are using the DSR Remote Operations software.

1. Select *Macros* - *Configure* - *Macro Groups* from the Video Viewer window menu.

   -or-

   Click the *Macro Groups* button.

   The Macros Groups dialog box appears.

2. Select one of the following:

   All - displays both Personal and Global macro groups.

   Personal - displays Personal Macro groups only.

   Global - displays Global Macro groups only.

3. Select the macro group to be altered from the Defined Groups list box. Windows and Sun are the default macro groups. If you have created new groups, they will also be displayed.
4. Click *Edit*. The Create/Edit Macro Groups dialog box will appear.
5. If you are editing a Personal Macro group, select one of the following from the View area:

   All- displays both personal and global macros.

   Personal - displays personal macros only.

   Global - displays global macros only.

6. To add macros to the group, select the macro to add from the Macros Available list. Click the *Add* button. The macro moves to the Macros in Group list. Use the *Move Up* and *Move Down* buttons to move the macro up or down in relation to the other macros.
7. To remove macros from the group, select the macro to delete from the Macros in Group list. Click the *Remove* button. The macro moves to the Macros Available list.
8. Repeat steps 6 and 7 until the Macros in Group list contains all the desired macros.
9. Click *OK* to accept the macro group and return to the Macro Groups dialog box.

   -or-

   Click *Cancel* to leave the dialog box without saving changes.

10. Click *Close* to exit the Macro Groups dialog box.

To rename a macro group:

NOTE: Macro groups cannot be renamed if you are using the DSR Remote Operations software.

1. Select *Macros* - *Configure* - *Macro Groups* from the Video Viewer window menu.

   -or-

   Click the *Macro Groups* button.

   The Macro Groups dialog box appears.
2. Select one of the following:

   All - displays both Personal and Global Macro groups.

   Personal - displays Personal Macro groups only.

   Global - displays Global Macro groups only.
3. Select the macro group to be altered from the Defined Groups list box. Windows and Sun are the default macro groups. If you have created new groups, they will also be displayed.
4. Click *Edit*. The Create/Edit Macro Groups dialog box will appear.
5. In the Macro Group Name field, enter a 1-32 character unique macro group name.
6. Click *OK* to save the name and return to the Macro Groups dialog box.

   -or-

   Click *Cancel* to leave the dialog box without saving changes.
7. Click *Close* to exit the Macro Groups dialog box.

To delete a macro group:

NOTE: Macro groups cannot be deleted if you are using the DSR Remote Operations software.

1. Select *Macros* - *Configure* - *Macro Groups* from the Video Viewer window menu.

   -or-

   Click the *Macro Groups* button.

   The Macro Groups dialog box appears.
2. Select one of the following:

   All - displays both Personal and Global Macro groups.

   Personal - displays Personal Macro groups only.

   Global - displays Global Macro groups only.
3. Select the macro group to be deleted from the Defined Groups list box.
4. Click the *Delete* button. You are prompted to confirm the deletion.
5. Click *Yes* to confirm or *No* to cancel the deletion.
6. Click *Close* to exit the Macro Groups dialog box.

To copy a macro group:

NOTE: Macro groups cannot be copied if you are using the DSR Remote Operations software.

1. Select *Macros* - *Configure* - *Macro Groups* from the Video Viewer window menu.

   -or-

   Click the *Macro Groups* button.

   The Macro Groups dialog box appears.
2. Select one of the following:

   All - displays both personal and global macros.

   Personal - displays personal macros only.

   Global - displays global macros only.
3. Select the desired macro from the Defined Groups list and then click *Copy.* The Copy Macro Group dialog box will appear.
4. Type a 1-32 character name in the Name of copied macro group field.
5. Select whether you wish to make the copied macro group a personal or global macro from the Macro Type area.
6. Click *OK* to copy the macro group. The Copy Macro Group dialog box is closed and the copied macro group will appear in the Macro Groups dialog box.

   -or-

   Click *Cancel* to cancel the action.
7. Click *Close* to exit the Macro Groups dialog box.

To change the macro group to be displayed in the Macros menu:

NOTE: The macro group displayed on the Macros menu cannot be changed if you are using the DSR Remote Operations software.

1. Select *Macros* - *Configure* - *Macro Groups* from the Video Viewer window menu.

   -or-

   Click the *Macro Groups* button.

   The Macro Groups dialog box appears.
2. Select one of the following:

   All - displays both Personal and Global Macro groups.

   Personal - displays Personal Macro groups only.

   Global - displays Global Macro groups only.
3. Select the macro group to be displayed from the Defined Groups list box.
4. Select *Display on Menu* if you wish for the macro group to appear in the Macros menu.
5. Click *Close* to exit the Macro Groups dialog box.

Macros in the selected group will appear in the Video Viewer window Macros menu.

To display a macro group:

NOTE: Macro groups cannot be displayed if you are using the DSR Remote Operations software.

Select *Macros - Display on Menu* and then select one of the macro groups Sun or Windows.

Power Controlling Target Devices

NOTE: You must have Appliance Administrator privileges to use the Tools - Power Control command. See *Built-in User Groups* on page 22 for more information.

If a target device is connected to an SPC device outlet, you may power up, power down or cycle (power up and then power down) the target device using the Power Control dialog box.

To power up a target device:

1. Select *Tools - Power Control* from the Video Viewer main window. The Power Control dialog box will appear.
2. Click the *Power On the Server* button. A warning dialog box will appear.
3. Click *OK* to confirm or *No* to cancel.
4. Click *Close* to close the dialog box.

To power down a target device:

1. Select *Tools - Power Control* from the Video Viewer main window. The Power Control dialog box will appear.
2. Click the *Power Off the Server* button. A warning dialog box will appear.
3. Click *OK* to confirm or *No* to cancel the command.
4. Click *Close* to close the dialog box.

To power cycle a target device:

1. Select *Tools - Power Control* from the Video Viewer main window. The Power Control dialog box will appear.
2. Click the *Power Cycle the Server* button. A warning dialog box will appear.
3. Click *OK* to confirm or *No* to cancel the command.
4. Click *Close* to close the dialog box.

Displaying Video Viewer Users

NOTE: This procedure is not available if the DSR Remote Operations software is being used.

You may select the *View - Connected Users* command or click the *Connected Users* button to display the current users connected to a Video Viewer window session.

To display current Video Viewer users:

1. Select *View - Connected Users* from the Video Viewer window menu.

   -or-

   Click the *Connected Users* button.

   The Users Connected to <device - Video Session number> dialog box appears, containing a list of all users connected to the Video Viewer window session.
2. Click *OK* to close the dialog box.

Saving the View

The display of a Video Viewer window may be saved to either a file or to the clipboard for pasting into a word processing or other program.

To capture the Video Viewer window to a file:

1. Select *File - Capture to File* from the Video Viewer window menu.

   -or-

   Click the *Capture to File* button.

   The Save As dialog box appears.
2. Enter a filename and choose a location to save the file.
3. Click *Save*.

To capture the Video Viewer window to your clipboard:

Select *File - Capture to Clipboard* from the Video Viewer window menu.

-or-

Click the *Capture to Clipboard* button.

The image data is saved to the clipboard.

Closing a Video Viewer Window Session

To close a Video Viewer window session:

Select *File - Exit* from the Video Viewer window.

Using Virtual Media

The virtual media feature allows the user on the client workstation to map a physical drive on that machine as a virtual drive on a target device. The client may also add and map an ISO or floppy image file as a virtual drive on the target device.

You may have one CD drive and one mass storage device mapped concurrently.

- A CD/DVD drive, disk image file (such as an ISO or floppy image file) is mapped as a virtual CD drive.
- A floppy drive, USB memory device or other media type is mapped as a virtual mass storage device.

Requirements

Virtual media is supported on DSR1030, 1031, 2030, 2035, 4030, 8030 and 8035 switches.

The target device must be connected to the DSR switch with a DSRIQ-USB2 module.

The target device must be intrinsically able to use the types of USB2-compatible media that you virtually map. In other words, if the target device does not support a portable USB memory device, you cannot map that on the client machine as a virtual media drive on the target device.

The user (or user group to which the user belongs) must have permission to establish virtual media sessions and/or reserved virtual media sessions to the target device. See *Changing Unit Access Rights* on page 102 for more information.

Only one virtual media session may be active to a target device at one time.

You may not use the virtual media feature with the DSR Remote Operations software.

Sharing and preemption considerations

The KVM and virtual media sessions are separate; therefore, there are many options for sharing, reserving or preempting sessions. The DSView software has the flexibility to accommodate the system needs.

For example, the KVM and virtual media sessions may be locked together. In this mode, when a KVM session is disconnected, so is the associated virtual media session. If the sessions are not locked together, the KVM session can be closed but the virtual media session will remain active. This could be desirable if a user is performing a time-intensive task using the virtual media session (such as an operating system load), and wants to establish a KVM session with a different target device to perform other functions while the operating system load progresses.

Once a target device has an active virtual media session without an associated active KVM session, two situations can occur - the original user (User A) can reconnect or a different user (User B) can connect to that channel. You may set an option in the Virtual Media dialog box (Reserved) that allows only the User A to access that channel with a KVM session.

If User B is allowed to access that session (the Reserved option is not enabled), User B could control the media that is being used in the virtual media session. In some environments, this may not be desirable.

By using the Reserved option in a tiered environment, only User A could access the lower switch and the KVM channel between the upper switch and lower switch would be reserved for User A.

Preemption levels offer additional flexibility of combinations. See *Launching an exclusive KVM session* on page 173 and *Connecting to an existing session* on page 173. The preemption modes described in those sections also apply to virtual media session.

Virtual Media dialog box

The Virtual Media dialog box is a program that manages the mapping and unmapping of virtual media. The dialog box displays all the physical drives on the client's workstation that can be mapped as virtual drives. You may also add ISO and floppy image files and then map them using the Virtual Media dialog box.

After a device is mapped, the Virtual Media dialog box Details View displays information about the amount of data transferred and the time elapsed since the device was mapped.

You may specify that the virtual media session is reserved. When a session is reserved, and the associated KVM session is closed, another user cannot launch a KVM session to that target device. If a session is not reserved, another KVM session may be launched.

You may also reset the USB2 IQ module from the Virtual Media dialog box. This action will reset every form of USB media on the target device, and should therefore be used with caution, and only when the target device is not responding.

Virtual media session settings

Virtual media session settings include locking, mapped drives access mode and encryption level. The procedure beginning on page 124 describes how to specify these settings for the supported DSR switch.

Table 6.4 lists and describes the virtual media session settings.

Table 6.4: Virtual Media Session Settings

Setting	Description
Locking	The locking option specifies whether a virtual media session is locked to the KVM session on the target device. When locking is enabled (which is the default) and the KVM session is closed, the virtual media session will also be closed. When locking is disabled and the KVM session is closed, the virtual media session will remain active.
Mapped drives access mode	You may set the access mode for mapped drives to read-only or read-write. When the access mode is read-only, the user will not be able to write data to the mapped drive on the client workstation. When the access mode is read-write, the user will be able to read and write data from/to the mapped drive. If the mapped drive is read-only by design (for example, certain CD/DVD drives or ISO images), the configured read-write access mode will be ignored. Setting the read-only mode can be helpful when a read-write drive such as a mass storage device or a USB removable media is mapped, and you wish to prevent the user from writing data to it.
Encryption level	You may configure up to three encryption levels (or none) for virtual media sessions. Any combination is valid. The choices are: DES, 3DES and 128-bit SSL. The default is no encryption (no encryption levels selected).

Opening a virtual media session

NOTE: The following procedures are valid only on DSR1030, 1031, 2030, 2035, 4030, 8030 and 8035 switches that are connected with DSRIQ-USB modules.

To launch a virtual media session:

From the Video Viewer toolbar, select *Tools* - *Virtual Media*. The Virtual Media dialog box will appear.

If you wish to make this a reserved session, click *Details*, then enable the *Reserved* checkbox.

To map a virtual media drives:

1. Open a virtual media session from the Video Viewer toolbar by selecting *Tools* - *Virtual Media.*
2. To map a physical drive as a virtual media drive:
   a. In the Virtual Media dialog box, click the *Mapped* checkbox next to the drive(s) you wish to map.
   b. If you wish to limit the mapped drive to read-only access, click the *Read Only* checkbox next to the drive. If the virtual media session settings were previously configured so that all mapped drives must be read only, this checkbox will already be enabled and cannot be changed.

      You might wish to enable the *Read Only* checkbox if the session settings enabled read and write access, but you wished to limit a particular drive's access to read only.
3. To add and map an ISO or floppy image as a virtual media drive:
   a. In the Virtual Media dialog box, click *Add Image*.
   b. The common file dialog box will appear, with the directory containing disk image files (that is, those ending in .iso or .img) displayed. Select the desired ISO or floppy image file and click *Open.*

      -or-

      If the client workstation's operating system supports drag-and-drop, select the desired ISO or floppy image file from the common file dialog box and drag it onto the Virtual Media dialog box.
   c. The file's header is checked to ensure it is correct. If it is, the common file dialog box will close and the chosen image file will appear in the Virtual Media dialog box, where it can be mapped by clicking the *Mapped* checkbox.
   d. Repeat steps a through c for any additional ISO or floppy images you wish to add. You may add any number of image files (up to the limits imposed by memory), but you may only have one virtual CD or virtual mass storage mapped concurrently.

   If you attempt to map too many drives (one CD and one mass storage device) or too many drives of a particular type (more than one CD or mass storage device), a message will be

displayed. If you still wish to map a new drive, you must first unmap an existing mapped drive, then map the new drive.

After a physical drive or image is mapped, it may be used on the target device.

To unmap a virtual media drive:

1. In the Virtual Media dialog box, uncheck the *Mapped* checkbox next to the drive you wish to unmap.
2. You will be prompted to confirm the unmapping. Click *Yes* to confirm or *No* to cancel.
3. Repeat for any additional virtual media drives you wish to unmap.

To display virtual media drive details:

In the Virtual Media dialog box, click *Details*. The dialog box expands to display the Details table. Each row indicates:

- Target Drive - Name used for the mapped drive, such as Virtual CD 1 or Virtual CD 2.
- Mapped to - Identical to Drive information that appears in the Client View Drive column.
- Read Bytes and Write Bytes - Amount of data transferred since the mapping.
- Duration - Elapsed time since the drive was mapped.

To close the Details view, click *Details* again.

To reset all USB devices on the target device:

NOTE: The USB reset feature resets every USB device on the target device, including the mouse and keyboard. It should only be used when the target device is not responding.

1. In the Virtual Media dialog box, click *Details*.
2. The Details View will appear. Click *USB Reset*.
3. A warning message will appear, indicating the possible effects of the reset. Click *Yes* to confirm the reset or *No* to cancel the reset.
4. To close the Details view, click *Details* again.

Closing a virtual media session

To close the Virtual Media dialog box:

1. Click *Exit*.
2. If you have any mapped drives, a message is displayed, indicating that the drives will be unmapped. Click *Yes* to confirm or *No* to cancel.

If a user attempts to disconnect a virtual media session or an active KVM session that has an associated locked virtual media session, a confirmation message is displayed, indicating that any virtual media mappings will be lost.

See *Sharing and preemption considerations* on page 201 and *Managing Active Sessions* on page 129 for information about other factors that may affect virtual media session closings.

Troubleshooting

If the Video Viewer or the Virtual Media dialog box does not start, the local Java cache may be corrupted. You can easily clear the cache without losing any data.

To clear the local Java cache:

1. Start the Java Control panel.

   On supported Windows systems, this will be an item in the Control Panel.

   On supported Linux systems, from a shell prompt, change directory to the bin directory where Java is installed. Then type **./ControlPanel**.

   For example:

   ```
   cd /usr/java/avocent/jrel.5.0_02/bin
   ./ControlPanel
   ```

2. Select the *General* tab.
3. Click the *Settings* button.
4. Click the *View Applications* button.
5. Select any *DSView Video Viewer Application* items.
6. Click the *Remove Selected Entries* button (this button may also be named *Remove Selected Application*).

If this does not solve the problem, repeat step 1, then click the *Delete Files* button.

NOTE: Clicking the Delete Files button will remove all applications installed with Java Web Start.

CHAPTER 7

Using the Telnet Viewer

The DSView management software ships bundled with a built-in proprietary Telnet Viewer that provides features unavailable in many other Telnet programs. These features include configurable session properties tailored for each device, configurable user preferences for all sessions, a scripting function for automatic device login, a macro function and a logging function.

About the Telnet Viewer

DSView software clients may use the DSView management software Telnet Viewer to access CPS810 and 1610 appliances and their ports, CCM 850, 1650 and 4850 appliances and their ports, or any generic appliance that supports Telnet Viewer connections.

NOTE: Throughout this chapter, the term “appliance” or “managed appliance” will be used to indicate a supported CPS appliance, CCM appliance or generic appliance that supports Telnet Viewer connections.

When a session is established with a supported CPS or CCM appliance, the Telnet client switches to SSH (Secure Shell) mode and opens an SSH shell to/through the appliance. The SSH shell can use any of the Telnet client’s terminal emulations. See *Security Property* on page 210 for more information.

The Telnet Viewer uses the credentials provided by the DSView management software to establish a session and will automatically accept the appliance server key. The username and password provided by the users when they log in are authenticated by the authentication service configured in the DSView software.

Requirements

The Telnet Viewer is actually an applet that runs within the Java 1.5.0_02 plug-in (JRE). The Telnet Viewer may also work with other Java versions. The DSView software client automatically downloads and installs the JRE (Java Runtime Environment) the first time the Video Viewer or the Telnet Viewer is launched. See *Java Installation* on page 47 for information about user interaction with the JRE installer.

Telnet Viewer Window Features

A new Telnet Viewer window will open for each new Telnet session established by a user. The Telnet Viewer window contains menus, a toolbar and a window that provides virtual terminal emulation. Figure 7.1 shows the Telnet Viewer and descriptions follow in Table 7.1.

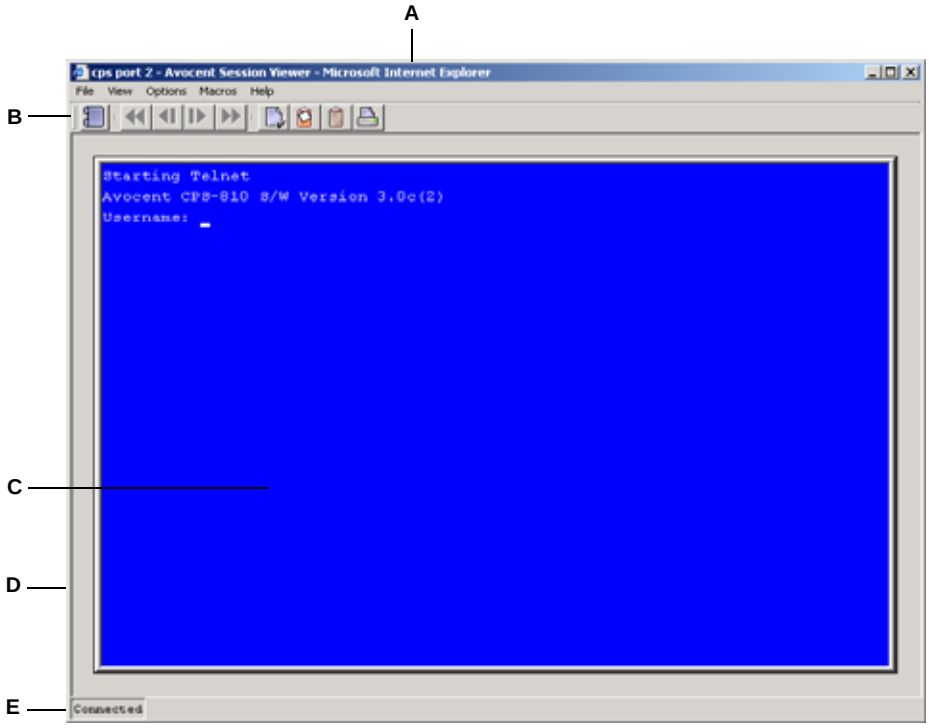


Figure 7.1: Telnet Viewer Window

Table 7.1: Telnet Viewer Window Descriptions

Letter	Description
A	Title Bar: Displays the name of the target device being viewed.
B	Toolbar: Allows you to access many of the features in the Telnet Viewer. See Table 7.2 for a description of the toolbar icons.
C	Virtual Terminal window: Interacts with your target device through this window. By default the window size is 80 characters x 24 lines.

Table 7.1: Telnet Viewer Window Descriptions (Continued)

Letter	Description
D	Viewer window: Resizes the window when you click and hold on the frame. Although the window may be resized, the Virtual Terminal window will remain the same size.
E	Status Bar: Displays one of the following: Connected - Displays during normal terminal emulation in a Telnet Viewer session Logging - Displays when logging is enabled Logging Paused - Displays when logging is paused

NOTE: The Close button may not be present on all operating systems.

Telnet Viewer window toolbar

Table 7.2 describes the Telnet Viewer window's toolbar icons.

Table 7.2: Telnet Viewer Window Toolbar Icons

Icon	Description
	Session Settings - Displays the Session Properties dialog box
	Help - Displays the DSView software help
	Copy Screen - Copies a screen of Telnet Viewer session data to the system clipboard
	Copy Buffer - Copies the contents of the Telnet Viewer session buffer to the system clipboard
	Copy Text - Copies highlighted text in a Telnet Viewer session screen to the system clipboard
	Restore - Restores the ability to highlight screen text when autoscaling is enabled and the virtual terminal window has been scaled
	Paste - Pastes the contents of the system clipboard into a Telnet Viewer session
	Prints a screen of Telnet Viewer session data

Security Property

A fully functional SSH2 (Secure Shell Version 2) Client is built into the Telnet Viewer. The SSH2 Client is Java-based and provides a secure method for accessing target devices.

The Telnet Viewer provides the following security features:

- Strict host key checking
- Support ciphers for AES (128-, 192-, 256-bit), Blowfish, Twofish, Cast, 3DES and Arcfour
- Diffie-Hellman key exchange support
- SSH-RSA key types
- Supported for hmac-md5, hmac-sha1, hmac-sha1-96, hmac-md5-96 and hmac-ripemd160

The DSView software will determine whether to create a Telnet or SSH2 connection when you start a session with an appliance. A serial connection provides SSH2 serial access to the target device from the appliance. Terminal emulation options are supported using both types of connections.

The SSH2 client is started when you initiate a session with an appliance port from the DSView Explorer. The DSView software server is contacted, which in turn contacts the target device connected to the appliance port and exchanges X.509 certificates with the target device. The target device also supplies a session certificate, private key and appliance certificate.

These certificates are then passed back to the SSH2 client, which uses them to determine the SSH2 host key and the user SSH2 key. The Telnet Viewer will then establish a session with the target device (or through the proxy server if there is a proxy server connection). The Telnet Viewer then passes the RSA public key from the session certificate when establishing the SSH connection. Finally, the virtual terminal window will open using an SSH2 shell over SSH connection.

SSH2 settings may be viewed by clicking on an appliance name in the DSView Explorer and selecting *Appliance Settings* - *Sessions* - *Settings* in the side navigation bar to display the Properties - Sessions - Settings window.

Opening a Session

A DSView management software Telnet Viewer session is opened using the DSView Explorer by clicking on *Telnet Session* or *Serial Session* in the Action column of the target device. If the target device is attached to an appliance port, Telnet Session will appear. If the target device is attached to an appliance that is also attached to a serial device, Serial Session will appear.

NOTE: If multiple connection methods are available, an alternate actions arrow will appear to the right of the action. Clicking the alternate action arrow will display a list of other actions, in descending order of priority, which may selected to launch the corresponding window type.

To open a Telnet Viewer session:

1. From the DSView Explorer, click the *Units* tab. *Units* will automatically be selected in the top navigation bar and *Unit Views* will automatically be selected in the side navigation bar.

2. From the side navigation bar, click a link to display the Appliances, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window.
3. In the Action column for the appliance, click *Telnet Session*. The Telnet Viewer window will appear.

   -or-

   In the Action column for the appliance, click *Serial Session*. The Telnet Viewer window will appear.

   -or-

   Click the alternate actions arrow in the Action column for the appliance and click either *Telnet Session* or *Serial Session*. The Telnet Viewer window will open.

   -or-

   Click on the name of the appliance you wish to view. *Overview* will automatically be selected and the name of the appliance will appear at the top of the side navigation bar. The Overview window will open.

NOTE: If a web browser address was defined when you added the appliance, Browser Session will appear in the Action column and you must use the Overview window or click the alternate actions arrow to open a Telnet Viewer window.

4. Click the *Telnet Session* icon or text.

   -or-

   Click the *Serial Session* icon or text.

   The Telnet Viewer window will open.

Customizing the Telnet Viewer

You may specify preferences that will be used for every Telnet Viewer session, regardless of the device to which you connect. These application preferences are entered from the Telnet Viewer window when you are connected to a device or port. After the preferences are entered, they are applied to devices/ports during subsequent sessions.

To change the window background and/or text color:

1. Select *Options - Preferences* from the menu bar. The Preferences dialog box will appear.
2. To change the background color, click the *Background/Normal Mode* box in the Colors section and select a color. The default color is blue.
3. To change the text color, click the *Text/Normal Mode* box in the Colors section and select a color. The default color is white.

To change the cursor appearance:

1. Select *Options - Preferences* from the menu bar. The Preferences dialog box will appear.

2. In the Caret list, choose *Block* to display the cursor as a block or choose *Underline* to display the cursor as an underline. The default value is Underline.

To enable/disable an exit warning prompt for Telnet Viewer sessions:

1. Select *Options - Preferences* from the menu bar. The Preferences dialog box will appear.
2. Enable or disable the *Prompt on Exit* checkbox. When the exit warning prompt is enabled, a message appears when you select *Telnet - Exit*. You may then choose to exit or continue the session. When disabled, the session closes without further prompting.The default value is enabled.

To enable/disable autoscaling:

1. Select *Options - Preferences* from the menu bar. The Preferences dialog box will appear.
2. Enable or disable the *Auto Scale* checkbox. When autoscaling is enabled, the user may reduce or expand the virtual terminal window by dragging a corner of the window. When autoscaling is disabled, the virtual terminal window will not scale when the view is changed; instead, scroll bars will appear around the window. The default value is enabled.

Customizing Session Properties

When you are connected to an appliance or port using the DSView management software Telnet Viewer, you may specify session properties that will be stored and reused every time you connect to the selected appliance or port. When you select *Options - Session Properties* in the DSView management software Telnet Viewer, the Session Properties dialog box will appear containing Terminal, Login Scripts and Logging tabs.

To change the terminal window size:

1. Select *Options - Session Properties* from the menu bar.

   -or-

   Click the *Session Settings* icon in the toolbar.

   The Session Properties dialog box will appear.
2. Click the *Terminal* tab.
3. In the Rows list, choose a value of *24* or *48*. The default value is 24.
4. In the Columns list, choose a value of *80* or *132*. The default value is 80.

To change the terminal emulation mode:

1. Select *Options - Session Properties* from the menu bar.

   -or-

   Click the *Session Settings* icon in the toolbar.

   The Session Properties dialog box will appear.
2. Click the *Terminal* tab.

3. From the Terminal Emulation list, choose one option. The default value is VT100. *Terminal Emulation* on page 311 contains encoding and decoding information for each of the terminal emulation types.

NOTE: When connecting to an appliance, the terminal type setting must match the terminal emulation type.

To change the Telnet Viewer Arrow key sequences:

When the Terminal Emulation mode is VT100, VT100+, VT102, VT52, VT220 or VT320, you may specify either VT100 or ANSI **Arrow** key sequences. Table 7.3 lists the **Arrow** keys and the sequences transmitted for each

Table 7.3: Arrow Key Sequences

Key	VT100	ANSI	VT52*
Up Arrow	<Esc> [A	<Esc> OA	<Esc> A
Down Arrow	<Esc> [B	<Esc> OB	<Esc> B
Right Arrow	<Esc> [C	<Esc> OC	<Esc> C
Left Arrow	<Esc> [D	<Esc> OD	<Esc> D

* When the Terminal Emulation mode is VT52, the **Arrow** keys are interpreted as indicated in this column, regardless of the value in the Arrow Keys list.

1. Select *Options - Session Properties* from the menu bar.

   -or-

   Click the *Session Settings* icon in the toolbar.

   The Session Properties dialog box will appear.
2. Click the *Terminal* tab.
3. In the Arrow Keys list, choose either *VT100* or *ANSI*. The default value is VT100.

To change the terminal type:

1. Select *Options - Session Properties* from the menu bar.

   -or-

   Click the *Session Settings* icon in the toolbar.

   The Session Properties dialog box will appear.
2. Click the *Terminal* tab.
3. In the Terminal Type box, enter a value of up to 40 characters, beginning with a letter and ending with a letter or digit. Valid characters are the letters A-Z, digits 0-9, forward slash,

dash, left parenthesis and right parenthesis. The terminal type must be entered in the Terminal Type field exactly as shown in Table 7.4.

Table 7.4: Terminal Emulation and Type

Terminal Emulation	Terminal Type
VT52	DEC-VT52
VT100	DEC-VT100
VT100+	DEC-VT100
VT102	DEC-VT102
VT220	DEC-VT220
VT320	DEC-VT320

To change the linefeed settings:

1. Select *Options - Session Properties* from the menu bar.

   -or-

   Click the *Session Settings* icon in the toolbar.

   The Session Properties dialog box will appear.
2. Click the *Terminal* tab.
3. When connecting to devices that do not insert a carriage return in incoming or outgoing data, automatically inserting a line after each line of data can prevent overwriting data when a new line is received.

   If the *New Line Mode - Inbound* box is checked, an inbound carriage return from the device will be treated as if both a carriage return and a linefeed were received. If not checked, a linefeed is not added to an inbound carriage return.

   If the *New Line Mode - Outbound* box is checked, an outbound carriage return to the device will always be followed by a linefeed character. If not checked, a linefeed is not sent with a carriage return. The default value is disabled for inbound and outbound.

To enable/disable line wrap:

1. Select *Options - Session Properties* from the menu bar.

   -or-

   Click the *Session Settings* icon in the toolbar.

   The Session Properties dialog box will appear.
2. Click the *Terminal* tab.
3. Enable or disable the *Auto wrap line* checkbox. When line wrap is enabled, characters wrap onto the next line when a new character is received and the cursor is at the end of the line.

When disabled, new characters will overwrite the last character on the current line when the cursor is at the end of the line. The default value is enabled.

To enable/disable local echo:

1. Select *Options* - *Session Properties* from the menu bar.

   -or-

   Click the *Session Settings* icon in the toolbar.

   The Session Properties dialog box will appear.
2. Click the *Terminal* tab.
3. When you are connected to a device that does not repeat or echo the data that you type, you may enable Local Echo mode. Otherwise, the Telnet Viewer will not display the text you type. However, if you are connected to a device that echoes data, and you are in Local Echo mode, all of the data you type will appear on your terminal twice.

   Enable or disable the *Local echo* checkbox. The default value is disabled.

To enable/disable 7-bit ASCII:

1. Select *Options* - *Session Properties* from the menu bar.

   -or-

   Click the *Session Settings* icon in the toolbar.

   The Session Properties dialog box will appear.
2. Click the *Terminal* tab.
3. Enable or disable the *Strip 8th bit* checkbox. The default value is disabled.

Login scripts

The DSView management software Telnet Viewer has a login scripting function that enables you to automatically log in to a device. A login script is built with a sequence of expect and send strings, and initial transmission characters that work with them. To use a login script, you must enable automatic login in a checkbox.

The first Initial character (that is, the first entry in the Initial character column) specifies what is sent to the device as soon as the Telnet Viewer session is established. This is selected from a list containing the choices: None, CR (carriage return), CR+LF (carriage return and linefeed), ESC (Escape) and CTRL+P (Control and P).

The first Expect string indicates what the device will send as its first prompt.

The first Send string indicates what the login script will send to the device after it receives the first Expect string.

You may then build additional Expect and Send strings according to what the particular device will prompt for and what will be sent in response.

To build a login script and enable/disable automatic login:

1. Select *Options - Session Properties* from the menu bar.

   -or-

   Click the *Session Settings* icon in the toolbar.

   The Session Properties dialog box will appear.
2. Click the *Login Scripts* tab.
3. Enable or disable the *Automate login* checkbox. The default value is disabled.
4. In the Initial Character list, select one option: CR (carriage return), CR+LF (carriage return and linefeed), ESC (Escape), CTRL+P (Control+P sequence, 0X10 in hex) or None (no initial transmission character).
5. In the Expect box, type the 1-32 alphanumeric character string that you expect from the device. Spaces are allowed.
6. In the Send box, type the 0-32 alphanumeric character string that you wish to send in response to the Expect string. Spaces are allowed, and a blank field is valid. A CR or CR+LF is appended to the string, based on the New Line Mode - Outbound setting.
7. Repeat the Expect and Send entries as needed, to a maximum of four each.

Reviewing Session Data

During a Telnet Viewer session, you may review the accumulated screen contents by using the scroll bar or the **Arrow** keys. To return to the current session location, press **Enter**. The size of the buffer containing session data that can be reviewed is configurable.

You may optionally choose to change the color of the text and/or the background when you are reviewing session data. When you return to the current session location, the colors will return to those specified in the Telnet Viewer's configuration (see *Customizing the Telnet Viewer* on page 211).

While you are reviewing collected data, new incoming data is buffered, but it will not be displayed until you return to the current session location. You may not enter outgoing data.

To change the maximum number of lines in the session buffer:

1. Select *Options - Session Properties* from the menu bar.

   -or-

   Click the *Session Settings* icon in the toolbar.

   The Session Properties dialog box will appear.
2. Click the *Terminal* tab.
3. In the History Buffer Size box, type a value from 1-1000. The default value is 256.

To change the background and/or text color when reviewing session data:

1. Select *Options* - *Preferences* from the menu bar. The Preferences dialog box will appear.
2. To change the background color, click the *Background/History Mode* box in the Colors section and select a color. The default color is blue.
3. To change the text color, click the *Text/History Mode* box in the Colors section and select a color. The default color is white.

Macros

NOTE: Three additional types of macros are available in the DSView management software. Exit macros, created within the DSView Explorer, reside on DS1800 digital switches and DSR switches and are used by by these switches. Global macros and personal macros are created using the Video Viewer window and are used with KVM sessions with target devices attached to DS1800 digital switches and DSR switches. None of these macros may be used or are compatible with a Telnet Viewer.

The DSView software Telnet Viewer has a macro function that allows you to create and use macros during Telnet Viewer sessions. A macro comprises a series of keystrokes that you define. Additionally, you may specify a hotkey in the macro's definition. When you define a macro and enable its inclusion in the Macros menu, you may execute the macro during a Telnet Viewer session either by selecting it from the Macros menu or by pressing the defined hotkey on your keyboard.

You may also define one or more global macro or personal macro groups, then add macros to the groups. Personal macro groups may be created by any user and are only available for use on the target device on which they are created. Global macros may only be created by a DSView software administrator and are available for use by any user on the DSView software system.

A macro may belong to more than one macro group or belong to both personal and global macro groups; however, a macro does not have to belong to a macro group. Selecting *Macros* - *Configure* - *Groups* takes you to the Configure Macro Groups dialog box which contains a list of defined macro groups from which you may select one group or all defined groups. The macros in the selected group(s) are then available for use during subsequent Telnet Viewer sessions with that device/port.

After defining a macro or a macro group, you may edit or delete it at any time. When you delete a macro or macro group, you are prompted for confirmation. When you change a macro group name, each macro belonging to the changed macro group is updated, but the change is not visible until the next Telnet Viewer session is established. When you delete a macro group, you delete only its name - the individual macros in the group are not affected.

To create a macro:

1. Select *Macros* - *Configure* - *Macros* from the menu bar. The Configure Macros dialog box appears.
2. Click the *Create* button. The Configure Macros dialog box expands to display an Edit Macro area.

3. In the Macro Name field, Type a 1-64 character name for the macro.
4. To define a hotkey for the macro, choose one from the Key list. To add a modifier to the hotkey, check the *Control*, *Shift* or *Alt* boxes. (A macro's hotkey is accessible only when the macro belongs to the active macro group.)
5. By default, the *Include in Menu* box is checked, indicating the macro will appear in the Macros menu. If you do not wish to include the macro in the Macros menu, uncheck this box. In this case, if the macro definition includes a hotkey, you will still be able to use the hotkey to run the macro, even if the macro's name does not appear in the Macros menu.
6. Type the macro string in the Keystrokes box. For non-printing and special character code sequences, use the following escape sequences:

   New line: \n

   Carriage return: \r

   Form feed: \f

   Horizontal tab: \t

   Backspace: \b

   Delay character (500 ms): \d

   Hexadecimal code sequence: \0x<NN>, where <NN> is the hexadecimal byte. For example, the **Ctrl+D** character sequence may be sent by using 0x04.

   Octal code sequence: \0<NNN>, where <NNN> is the octal byte. For example, the **Ctrl+D** character sequence may be sent by using 0004.
7. From the Control Code drop-down menu, select the sequence you wish to invoke with the selected characters.
8. In the Access Rights area, specify whether you wish for the macro to be a global macro (available to all users) or a personal macro (available only to the current user).

   You must have DSView software administrator privileges to use the Access Rights area.
9. Click *OK*. The Configure Macros dialog box returns to its abbreviated display and the macro appears in the Macros area.
10. Click *OK* to close the Configure Macros dialog box.

To edit an existing macro:

NOTE: You must have DSView software administrator privileges to edit Global Macros.

1. Select *Macros* - *Configure* - *Macros* from the menu bar. The Configure Macros dialog box appears.
2. In the Macros table, select the macro you wish to edit.
3. Click the *Edit* button. The Configure Macros dialog box expands to display an Edit Macro area containing the information defined for the macro.
4. Edit the macro properties as needed.

5. Click *OK*. The changes are saved and the Configure Macros dialog box returns to its abbreviated view.
6. Repeat steps 2-5 to edit additional macros.
7. Click *OK* to close the Configure Macros dialog box.

To delete a macro:

NOTE: You must have DSView software administrator privileges to delete Global Macros.

1. Select *Macros* - *Configure* - *Macros* from the menu bar. The Configure Macros dialog box appears.
2. Select the macro in the Macros table that you wish to delete.
3. Click the *Delete* button. A dialog box appears, prompting you to confirm the deletion.
4. Click *Yes* to confirm or *No* to cancel the action.

To use a macro:

1. Select the macro from the Macros menu.

   -or-

   If the macro's definition includes a hotkey, press the hotkey or hotkey sequence. A macro's hotkey is accessible only when the macro belongs to the active macro group.

   -or-

   Select *Macros* - *Configure* - *Macros* from the menu bar.

   The Configure Macros dialog box appears.
2. Select the macro in the Macros table that you wish to run.
3. Click *Run*.

To create a macro group:

1. Select *Macros* - *Configure* - *Groups* from the menu bar. The Configure Macro Groups dialog box appears.
2. Click the *Create* button. The Configure Macros dialog box expands to display a Create Group area.
3. In the Group Name field, type a 1-64 character name for the macro group.
4. Select the macros you wish to add or remove to or from the macro group.

   To add macros to the macro group:

   - Select the macro you wish to add from the Macros Available list. Multiple macros may be selected by pressing **Ctrl** while clicking on the macro names.
   - Click *Add*. The macros will be moved to the Macros In Group list.

   To remove macros from the macro group:

- Select the macro you wish to remove from the Macros In Group list. Multiple macros may be selected by pressing **Ctrl** while clicking on the macro names.
- Click *Remove*. The macros will be moved to the Macros Available list.

5. In the Access Rights area, specify whether you wish for the macro group to be a Global Macro group (available to all users) or a Personal Macro group (available only to the current user).

   You must have DSView software administrator privileges to use the Access Rights area.
6. Click *OK*. The Configure Macro Groups dialog box returns to its abbreviated view.
7. Click *OK* to close the Configure Macro Groups dialog box.

To enable a macro group for use during Telnet Viewer sessions:

NOTE: You must have DSView software administrator privileges to enable a macro group.

1. Select *Macros* - *Configure* - *Groups* from the menu bar. The Configure Macro Groups dialog box appears.
2. In the Macro Groups table, select the macro group you wish to enable.
3. Click the *Edit* button. The Configure Macro Groups dialog box expands to display an Edit Group area containing the information defined for the macro.
4. Enable the *Active Group* checkbox.
5. Click *OK*. The changes are saved and the Configure Macro Groups dialog box returns to its abbreviated view.

To edit an existing macro group:

NOTE: You must have DSView software administrator privileges to edit Global Macro groups.

1. Select *Macros* - *Configure* - *Groups* from the menu bar. The Configure Macro Groups dialog box appears.
2. In the Macro Groups table, select the macro group you wish to edit.
3. Click the *Edit* button. The Configure Macro Groups dialog box expands to display an Edit Group area containing the information defined for the macro.
4. Edit the macro group properties as needed.
5. Click *OK*. The changes are saved and the Configure Macro Groups dialog box returns to its abbreviated view.
6. Repeat steps 2-5 to edit additional macro groups.
7. Click *OK* to close the Configure Macro Groups dialog box.

To delete a macro group:

NOTE: You must have DSView software administrator privileges to delete Global Macro groups.

1. Select *Macros* - *Configure* - *Groups* from the menu bar. The Configure Macro Groups dialog box appears.

2. Select the macro group in the Macro Groups table that you wish to delete.
3. Click the *Delete* button. A dialog box appears, prompting you to confirm the deletion.
4. Click *Yes* to confirm or *No* to cancel.

Logging

The Telnet Viewer has a logging function that saves the contents of a Telnet Viewer session to a file. You may enable automatic logging or dynamically start logging at any time. Additionally, you may pause, resume and stop logging, regardless of whether it was started automatically or dynamically.

While logging is occurring or when it is paused, a Logging Status label appears in the status panel at the bottom of the DSView management software Telnet Viewer window.

NOTE: When you enable or disable automatic logging, the logging will begin or end at the start of the next DSView software Telnet Viewer session to that device. If you change the default log file directory used for automatic logging, the change does not take effect until the next session to that device.

Log files

The format of log filenames is shown below, where <mmddyy> represents the month, day and year, and <hhmmss> represents the current hour, minute and second in military time:

scvTelnet<mmddyy>_<hhmmss>.log

The default log directory is session-specific, that is, each Telnet Viewer session may have its own location for storing logfiles. You may change the name of the file and the location of the directory that stores the logfiles. If you do not change the default directory, logfiles are stored in your home directory.

You may display a log file at any time, using a standard text editor. The screen buffer is written to the log file when the buffer is full, or when logging is paused or stopped. To ensure the log file is up-to-date, either pause or stop the logging.

To change the default log file directory:

1. Select *Options - Session Properties* from the menu bar.

   -or-

   Select the *Session Settings* icon in the toolbar.

   The Session Properties dialog box will appear.
2. Click the *Logging* tab. The Default Directory field displays the current default location for logfiles.
3. Click the *Browse* button. The Set Directory dialog box appears.
4. Select a directory from the Look in list.

   -or-

   Create a new directory:

a. Click the *Create New Folder* button. A new directory named New Folder appears in the directory list.

b. Click the *New Folder* entry in the directory list to highlight it. Then, click the entry again to edit its name. Type in a new name. Press **Enter**. The directory appears in alphabetical order in the directory list.

c. Select the newly-created directory in the directory list. The Filename field will now contain the name of the new directory.

5. Click the *Set Directory* button to select the newly-created or selected directory as the default log file directory. The Set Directory dialog box will close.
6. The Default Directory field now contains the name of the newly-created or selected directory. Click *OK* to save the new information.

   -or-

   Click *Cancel* to exit the dialog box without saving any new information.

To enable automatic logging:

1. Select *Options - Session Properties* from the menu bar.

   -or-

   Click the *Session Settings* icon in the toolbar.

   The Session Properties dialog box will appear.
2. Click the *Logging* tab.
3. Enable the *Logging* checkbox.
4. The Default Directory field displays the current default location for logfiles. If that is the desired directory, click *OK*. If you wish to change the default log file directory, see *To change the default log file directory:* on page 221.

Automatic logging will begin when you initiate the next DSView management software Telnet Viewer session to that device. At that time, the Logging Status label will indicate *Logging*.

To disable automatic logging:

1. Select *Options - Session Properties* from the menu bar.

   -or-

   Click the *Session Settings* icon in the toolbar.

   The Session Properties dialog box will appear.
2. Click the *Logging* tab.
3. Disable the *Logging* checkbox.
4. Click *OK*.

Automatic logging will stop when you close the Telnet Viewer session. When logging stops, the Logging Status label disappears.

To start dynamic logging:

1. Select *Options - Logging - Start* from the menu bar. The Log dialog box appears.
2. The Look in list contains the default log file directory and the Filename field contains the default log filename. Using this filename format is recommended; however, you may change it for the duration of this DSView management software Telnet Viewer session. If you choose to use the default log filename, skip to step 4.
3. To change the default log filename for the duration of the dynamic logging session, you may select a directory from the Look in list. The directory list may contain directories and files. To create a new directory:
   a. Click the *Create New Folder* button. A new directory named New Folder appears in the directory list.
   b. Click the *New Folder* entry in the directory list to highlight it. Then click the entry again to edit its name. Type in a new name. Press **Enter**. The directory appears in alphabetical order in the directory list.
   c. Double-click the newly-created directory in the directory list. The Filename field will now contain the name of the new directory.
   d. Type a new filename in the Filename field. If you enter a filename that already exists, the new file will overwrite the old file.
4. You are prompted to confirm the directory selection and begin logging. Click *Log* to confirm or *Cancel* to cancel.

When logging begins, the Logging Status label will indicate *Logging*.

To pause logging:

Select *Options - Logging - Pause* from the menu bar. The Logging Status label will change to *Logging Paused*.

To resume logging:

Select *Options - Logging - Resume* from the menu bar. The Logging Status label will change to *Logging*.

To stop logging:

Select *Options - Logging - Stop* from the menu bar. The Logging Status label will disappear.

Copying, Pasting and Printing Session Data

In the Telnet Viewer you may:

- Copy a screen of Telnet Viewer session data to the system clipboard
- Copy all of the Telnet Viewer session buffer contents to the system clipboard
- Copy a highlighted portion of the Telnet Viewer session data to the system clipboard

- Paste the contents of the system clipboard into a Telnet Viewer session or into another application
- Print a screen of the Telnet Viewer session data

Information that is copied from a DSView software Telnet Viewer session may be pasted into other applications. Similarly, information copied from other applications may be pasted into a Telnet Viewer session.

NOTE: Only textual data may be copied and pasted in the DSView software Telnet Viewer.

To copy a Telnet Viewer session window screen:

Select *Options* - *Copy Screen* from the menu bar.

-or-

Click the *Copy Screen* icon in the toolbar.

The screen contents will be saved to the system clipboard. You may then paste the clipboard contents into a Telnet Viewer session or into another application.

To copy all of the Telnet Viewer session buffer contents:

Select *Options* - *Copy Buffer* from the menu bar.

-or-

Click the *Copy Buffer* icon in the toolbar.

The entire buffer will be copied to the system clipboard (regardless of the amount of data in it. You may then paste the clipboard contents into a Telnet Viewer session or into another application.

To highlight and copy a portion of a Telnet Viewer window screen:

NOTE: When autoscaling has been enabled and the window has been scaled, you will not be able to highlight text until you click the *Restore* icon in the toolbar.

1. Use the mouse to drag-select the portion of the screen text you wish to copy.
2. Select *Options* - *Copy Text* from the menu bar.

   -or-

   Click the *Copy Text* icon in the toolbar.

   -or-

   Right-click and select *Copy Text* from the pop-up menu.

The highlighted text will be copied to the system clipboard. You may then paste the clipboard contents into a Telnet Viewer session or into another application.

To paste system clipboard contents:

1. Place textual data on the system clipboard, using a text editor or other application.
2. Initiate a Telnet Viewer session.

3. At the point where you wish to paste the clipboard contents, select *Options* - *Paste* from the menu bar.

   -or-

   Click the *Paste* icon in the toolbar.

To print a Telnet Viewer window screen:

1. Select *Options* - *Print Screen* from the menu bar.

   -or-

   Click the *Print Screen* icon in the toolbar.
2. The operating system's print dialog box appears. Make the appropriate settings. The screen contents will then be sent to the printer.

Power Controlling Target Devices (Serial Session Only)

NOTE: A user must have DSView software administrator privileges to control the power of a target device.

If a target device attached to an appliance port is connected to an SPC device outlet and the target device has been accessed in a serial session, you may power up, power down or cycle (power down and then power up) the target device using the Power Control dialog box. The Options - Power menu option will not be available if the target device cannot be power controlled using the DSView management software, or if the user does not have power control privileges (specified by selecting *Reboot Appliance* in the Unit Access Rights window).

The current state of the SPC device outlet appears in the Current Power Status area of the dialog box. As you change the power state, the information is updated in real time.

Depending on the configuration of an SPC device outlet, an SPC device outlet may not immediately respond to a power change request (for example, an SPC device outlet may be configured to remain off for a specific period of time, and so on).

To power up a target device:

1. Select *Options* - *Power* from the Video Viewer main window. The Power Control dialog box will appear.
2. Click *On*.
3. Click *Close* to close the dialog box.

To power down a target device:

1. Select *Options* - *Power* from the Video Viewer main window. The Power Control dialog box will appear.
2. Click *Off*.
3. Click *Close* to close the dialog box.

To power cycle a target device:

1. Select *Options* - *Power* from the Video Viewer main window. The Power Control dialog box will appear.
2. Click *Cycle*.
3. Click *Close* to close the dialog box.

Closing a Telnet Viewer Session

To close a Telnet Viewer session:

Select *File* - *Exit* from the Telnet Viewer window.

CHAPTER 8

Working with IPMI 1.5 Target Devices

An IPMI 1.5 target device is a server containing one or more BMCs (Baseboard management controllers) that are used to monitor internal sensor information such as temperature, fan speed and battery voltage. The BMCs in IPMI 1.5 target devices are added to your DSView software system using a DSI5100 IPMI proxy appliance, which provides a secure interface to all IPMI 1.5 target devices in your enterprise. The DSI5100 appliance is used to access, aggregate and report information from sensors read by the BMCs.

Sensor information may be viewed either graphically using the IPMI Viewer window, or by clicking on an IPMI 1.5 target device in a Unit Views window.

Adding and Changing DSI5100 Appliance BMCs

NOTE: You must have Configure Unit Settings rights to customize DSI5100 appliance BMC settings. See *Changing Unit Access Rights* on page 102 for more information.

BMCs accessed by a DSI5100 appliance are managed using the Appliance BMC Ports window. You may choose to add or remove BMCs or change the name, IP address, or username and password of a BMC.

To change an existing BMC, you must first click on the name of the DSI5100 appliance to which it is associated in a Unit Views window. Next, from the side navigation bar, click *Appliance Settings* and then *BMCs* to display the Appliance BMC Ports window. All BMCs associated with the DSI5100 appliance will appear in the Appliance BMC Ports window.

Information related to the IPMI 1.5 target device may be edited by clicking on the IPMI 1.5 target device in a Target Devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window. Overview, Properties, Access Rights and Connections information is modified similarly to that of non-IPMI 1.5 target devices. See *Managing Units* on page 95 for more information.

Click on the name of a BMC to change it using the links in the side navigation bar. The identity and credentials BMC settings may be viewed and modified.

Adding BMCs for use with a DSI5100 appliance

To add an IPMI 1.5 target device:

1. Click *Add* in the Appliance BMC Ports window. The Add IPMI BMC Wizard will appear. Click *Next*.
2. The Select a Target Device Option window will open.
   a. Click *Browse for an existing target device* if you wish to associate the BMC with an existing target device.

      -or-

      Click *Create a new target device* and type a name for the target device to which the BMC is attached.

NOTE: Only DSView software administrators and appliance administrators may create a new target device. If you are not a member of one of these groups, the Select a Target Device Option window will not appear. Instead, the Select a Target Device window will open and you must browse to select an existing target device to which you have Configure Unit Settings rights.

   b. Click *Next*.

   If you selected *Browse* for an existing target device, continue to step 3.

   -or-

   If you selected *Create* a new target device, go to step 4.
3. The Select a Target Device window will open. Select an IPMI 1.5 target device from the list, then click *Next*.
4. The Enter the BMC Address window will open. Type the IP address, in standard dot notation (xxx.xxx.xxx.xxx), for the BMC, then click *Next*.
5. The Enter BMC Credentials window will open.
   a. If required, type a username (0-16 characters) that will be used for communication with the BMC.
   b. If required, type a password (0-16 characters) that will be used for communication with the BMC.
   c. Click *Next*.
6. The Adding BMC window will open, followed by the Completed Successful window.
7. Click *Finish.*

Customizing the Appliance BMC Ports window

By default, the following fields display in the Appliance BMC Ports window:

- Name - The name of the BMC. You may click on a name to display and change BMC information.
- Address - The BMC IP address in standard dot notation (xxx.xxx.xxx.xxx).

The following fields are not displayed by default, but may be displayed using the Customize link:

- Username - The username that will be used when communicating with the BMC.
- Privilege Level - The privilege level of the BMC user, as specified in the BMC (administrator and so on).

See *Using the Customize link in windows* on page 15 for more information.

To display or change BMC identity settings:

1. Click *Appliance Settings* in the side navigation bar, and then click *BMCs*. The Appliance BMC Ports window will open.
2. Click on the name of a BMC port. *Identity* will automatically be selected in the side navigation bar and the BMC Identity window will open. The name of the BMC port will also appear under the DSI5100 appliance name in the side navigation bar.
3. Type a new name for the BMC.
4. Type the IP address, in standard dot notation (xxx.xxx.xxx.xxx), for the BMC.
5. Click *Save* and then click *Close*. The Appliance BMC Ports window will open.

To display or change BMC credentials:

1. Click *Appliance Settings* in the side navigation bar, and then click *BMCs*. The Appliance BMC Ports window will open.
2. Click on the name of a BMC port. *Identity* will be automatically selected in the side navigation bar and the BMC Identity window will open. The name of the BMC port will also appear beneath the DSI5100 appliance name in the side navigation bar.
3. Click *Credentials* in the side navigation bar. The BMC Credentials window will open.
4. Type a new username (0-16 characters) that will be used for communication with the BMC. If this field is left blank, anonymous authentication will be used for communication with the BMC.
5. Type a new password (0-16 characters) that will be used for communication with the BMC. If this field is left blank, anonymous authentication will be used for communication with the BMC.
6. Click *Save* and then click *Close*. The Appliance BMC Ports window will open.

To delete BMCs:

NOTE: Users must have Configure Unit Settings rights to delete BMCs. See *Changing Unit Access Rights* on page 102 for more information.

1. Click *Appliance Settings* in the side navigation bar, and then click *BMCs*. The Appliance BMC Ports window will open.
2. Click the checkbox to the left of the BMC you wish to delete.

   -or-

   Click the checkbox to the left of Name at the top of the list to select all BMCs listed in the window for deletion.

3. Click *Delete*. A confirmation dialog box will appear.
4. Click *OK* to confirm or *Cancel* to cancel.

Displaying Sensor Information Using the IPMI Viewer

The IPMI Viewer window is used to graphically display reported sensor information in the DSView management software. When you click *IPMI Session* in a Unit View window, the IPMI Viewer window appears in a separate web browser window.

The information graphically displayed using gauges in the IPMI Session window may vary between IPMI 1.5 target devices, due to the type of sensors in the BMC. For example, if a BMC does not contain a sensor that displays voltage information, that gauge will not appear in the IPMI Viewer window. You may specify how often information is refreshed in the IPMI Viewer window.

Launching an IPMI Viewer session

An IPMI session is launched from the DSView Explorer or using the Unit Overviews window.

To launch an IPMI session from the DSView Explorer:

1. Display a Target Devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window. See *About Unit Views* on page 81 for more information.
2. Click the *IPMI Session* link in the Action column of the target device you wish to view. The IPMI Viewer window launches in a new web browser window.

To launch an IPMI session using the Unit Overview window:

1. Display a Target Devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window. See *About Unit Views* on page 81 for more information.
2. Click on the name of a target device connected to a DSI5100 appliance. The side navigation bar will contain the name of the target device at the top and *Overview* will automatically be selected. The Unit Overview window will open.
3. Click on the *IPMI Session* name or icon.

The IPMI Viewer window launches in a new web browser window.

IPMI Viewer Window features

Figure 8.1 shows the IPMI Viewer window areas.

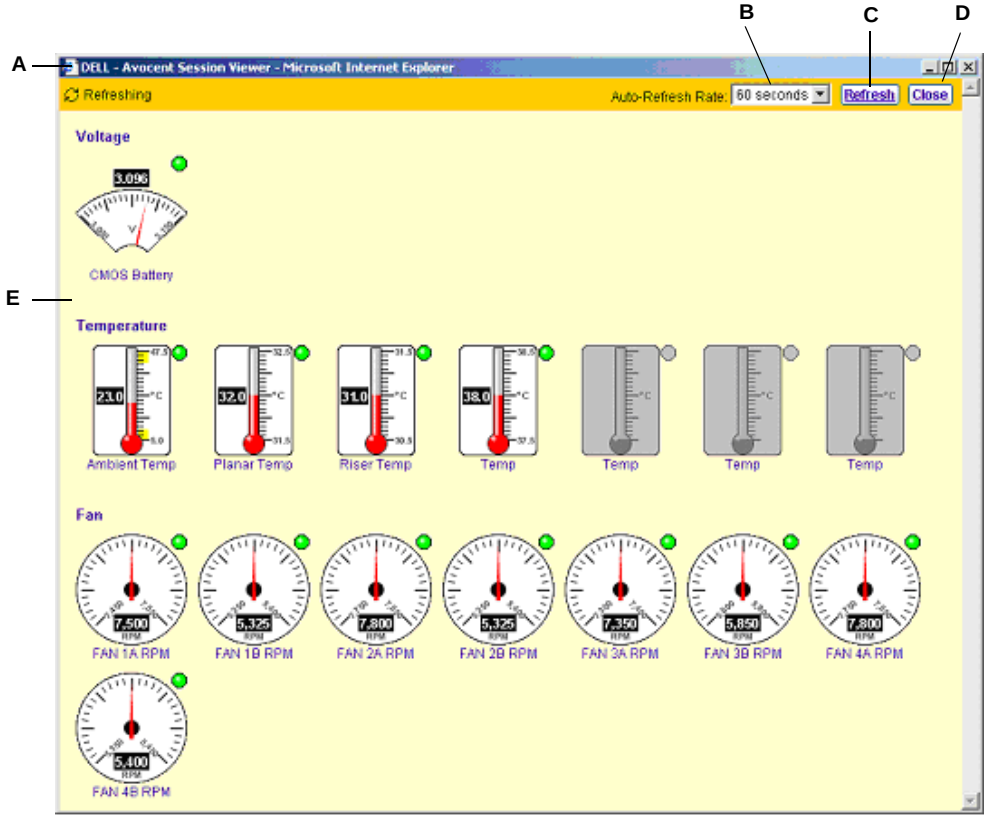


Figure 8.1: IPMI Viewer Window

Table 8.1 describes the IPMI Viewer window areas.

Table 8.1: IPMI Viewer Window Descriptions

Letter	Description
A	Title Bar: Displays the name of the IPMI 1.5 target device being viewed.
B	Auto-Refresh Rate: Allows you to specify how often the IPMI Viewer window gauges are updated. The default value is 60 seconds
C	Refresh: Manually updates the IPMI Viewer window gauges.
D	Close: Closes the IPMI Viewer window.

Table 8.1: IPMI Viewer Window Descriptions (Continued)

Letter	Description
E	IPMI Viewer display area: Contains gauges that display numeric readings from the BMC sensors in the IPMI 1.5 target device. Depending on the sensors on the BMC, any of the following gauges may appear in the IPMI Viewer window: Voltage - The voltages in the IPMI 1.5 target device. Current - The currents in the IPMI 1.5 target device. Fans - The revolutions per minute (RPM) of each fan in the target device. Temperature - The temperatures in the IPMI 1.5 target device, in degrees Celsius, including ambient, planar and riser temperature. Each gauge contains a status icon to its upper left, see Table 8.2

Table 8.2 describes the status icons that may appear in the IPMI Viewer window.

Table 8.2: IPMI Viewer Window Status Icons

Icon	Description
	(green circle) The current value is within acceptable threshold values.
	(grey circle) The current value is unknown.
	(yellow exclamation) The current value is in the non-critical area.
	(red x) The current value is in the critical area.
	(dark red sad face) The current value is in the non-recoverable area.

Gauges may also contain color areas at their upper and lower thresholds, as listed in Table 8.3.

Table 8.3: Upper and Lower Threshold Gauge Colors

Color	Description
Yellow	Non-critical threshold values
Red	Critical threshold values
Dark red	Non-recoverable threshold values

In Figure 8.2, the temperature gauge contains threshold values of approximately 5.0-9.25 at its lower threshold and approximately 43.25-47.5 at its upper threshold.

NOTE: Unsupported numeric sensor thresholds will not appear in the IPMI Viewer window.

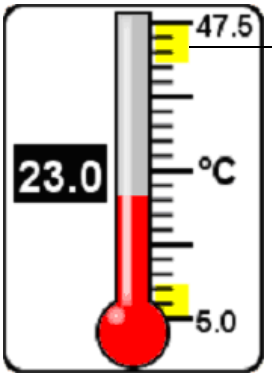


Figure 8.2: Upper and Lower Threshold Values

Refreshing the IPMI Viewer window

To specify an automatic refresh rate for the IPMI Viewer window:

From the IPMI Viewer window, select one of the following refresh rates: 30 seconds, 60 seconds or 90 seconds.

-or-

Select *Continuous* to update in real-time the values that dynamically change in the IPMI 1.5 target device BMC.

-or-

Select *Never* to prevent the gauges from automatically refreshing.

To refresh the IPMI Viewer window manually:

Select the *Refresh* button.

Closing an IPMI Viewer window

To close the IPMI Viewer window:

Select the *Close* button.

Displaying Sensor Information by Selecting an IPMI 1.5 Target Device

NOTE: To display IPMI 1.5 target device information, a user must be individually assigned rights or belong to a user group assigned rights to the IPMI 1.5 target device using the Unit Access Rights window. See *Changing Unit Access Rights* on page 102 for more information.

You may display information related to a supported IPMI 1.5 target device, including general information about the target device, the target device LAN configuration, field replaceable units

(FRUs) in the target device, in addition to discrete and numeric sensor information and system events read from the BMC.

Clicking the name of a supported IPMI 1.5 target device in a target devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window will display an IPMI link in the side navigation bar. Clicking the *arrow* next to IPMI will display a list of sub-links and automatically select the *Device Info* link and the IPMI Device Information window.

The following sub-links appear beneath the IPMI link when it is expanded. Clicking one of the sub-links in the side navigation bar performs the following actions:

- Device Info - Displays the IPMI Device Information window
- LAN Configuration - Displays the IPMI LAN Configuration window
- FRU Info - Displays the Field Replaceable Unit Information window
- Discrete Sensors - Displays the IPMI Discrete Sensors window
- Numeric Sensors - Displays the IPMI Numeric Sensors window
- SEL - Displays the System Event Log window

Displaying IPMI 1.5 target device BMC information

The IPMI Device Information window displays information for all BMCs in the IPMI 1.5 target device. The following information will appear for each BMC:

- IPMI Version - IPMI version with which the BMC is compatible.
- Firmware Version - BMC firmware version.
- SDR Version - Sensor data record (SDR) command set version of the SDR device.
- Manufacturer ID - Original equipment manufacturer (OEM) of the functionality in the BMC, including commands, codes and interfaces.
- Product ID - Manufacturer-specified identification used to specify the type of board, module or system in which the BMC is used.
- Device Revision - Firmware revision of the BMC.

To display IPMI 1.5 target device BMC information:

1. From a Target Devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window, click on the name of a IPMI 1.5 target device. The side navigation bar will contain the name of the target device at the top and *Overview* will automatically be selected. The Unit Overview window will open.
2. Click *IPMI* in the side navigation bar. Device Info will automatically be selected and the IPMI Device Information window will open.
3. Click *Close* when you are finished, to return to the Target Devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window.

Displaying LAN configuration information

The BMC LAN Configuration window displays information related to all BMCs in the IPMI 1.5 target device. The following information will appear for each BMC:

- IP Address - BMC IP address in standard dot notation (xxx.xxx.xxx.xxx).
- LAN MAC - BMC MAC address.
- Default Gateway IP - IP gateway (router) address used to send BMC messages or alerting a party on a different subnet.
- Default Gateway MAC - MAC gateway (router) address used to send BMC messages or alerting a party on a different subnet.

The following information may also appear for each configured BMC:

- Backup Gateway Address - Alternate gateway (router) IP address used to send LAN alerts.
- Backup MAC Address - Alternate gateway (router) MAC address used to send LAN alerts.

To display LAN configuration information:

1. From a Target Devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window, click on the name of a supported IPMI 1.5 target device. The side navigation bar will contain the name of the target device at the top and *Overview* will automatically be selected. The Unit Overview window will open.
2. Click *IPMI* in the side navigation bar and then click *LAN Config*. The BMC LAN Configuration window will appear.
3. Click *Close* when you are finished, to return to the Target Devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window.

Displaying field replaceable unit (FRU) information

The Field Replaceable Unit Information window displays information related to the FRU boards in the IPMI 1.5 target device. Any of the following information may appear for each configured FRU board.

- Chassis information - type, part number and serial number
- Board information - language (for example, English), manufacture date, manufacturer, product name, serial number, part number and file version (file used to load the FRU information on the board)
- Product information - language (for example, English), manufacturer, name, part model number, version, product serial number, asset tag and file version (file used to load the FRU information to the board)

To display FRU information:

1. From a Target Devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window, click on the name of a supported IPMI 1.5 target device. The side navigation

bar will contain the name of the target device at the top and *Overview* will automatically be selected. The Unit Overview window will open.

2. Click *IPMI* in the side navigation bar, and then click *FRU Info*. The Field Replacement Unit Information window will open.
3. Click *Close* when you are finished, to return to the Target Devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window.

Displaying IPMI 1.5 target device discrete sensor information

The IPMI Discrete Sensors window displays information about the discrete sensors managed by the BMCs in the IPMI 1.5 target device.

The type and number of sensors displayed will vary by BMC, motherboard and chassis implementation.

To display detailed information about a specific sensor managed by a BMC, click on its name. The IPMI Discrete Sensor Details window will open.

The following information appears in the IPMI Discrete Sensor Details window about the selected sensor:

- Name - Discrete sensor name.
- Sensor Type - Discrete sensor type.
- Reading Type - Discrete sensor reading type.
- Status - Discrete sensor items list and the state of each. A green check mark to the right of an item indicates an active state and a red X indicates a not active state.
- A red x will appear to the right of items for which the indicated action has not been taken.

Customizing the IPMI Discrete Sensors window

The Name field is always displayed in the IPMI Discrete Sensors window. An icon representing the discrete sensor type will appear to the left of the name. Clicking on the name of the discrete sensor or its icon will display the IPMI Discrete Sensor Detail window.

By default, the Status field is displayed and may be removed by using the Customize link.

The Sensor Type and Reading Type fields are not displayed by default, but may be displayed using the Customize link:

See *Using the Customize link in windows* on page 15 for more information.

To display IPMI 1.5 target device sensor information:

1. From a Target Devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window, click on the name of a supported IPMI 1.5 target device. The side navigation bar will contain the name of the target device at the top and *Overview* will automatically be selected. The Unit Overview window will open.
2. Click *IPMI* in the side navigation bar, and then click *Discrete Sensors*. The IPMI Discrete Sensors window will appear.

3. Click on the name of a sensor. The IPMI Discrete Sensor Details window will open.
4. Click *Close* when you are finished to return to the IPMI Discrete Sensors window.
5. Click *Close* when you are finished to return to the Target Devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window.

Displaying IPMI 1.5 target device numeric sensor information

The IPMI Numeric Sensors window displays information about the numeric sensors managed by the BMCs in the IPMI 1.5 target device.

The type and number of sensors displayed will vary by BMC, motherboard and chassis implementation.

To display detailed information about a specific sensor managed by a BMC, click on its name. The IPMI Numeric Sensor Details window will open.

The following information appears in the IPMI Numeric Sensor Details window about the selected sensor:

- Name - Numeric sensor name.
- Sensor Type - Numeric sensor type. A gauge icon representing the numeric sensor type will appear to the left of the name.
- Units - Numeric sensor type units (volts, RPM and so on).
- Current Reading - Numeric sensor current reading (5.006V, 35.0°C and so on).
- Status - Numeric sensor status. Possible status values are: OK, Non-Critical (Low), Critical (Low), Non-Recoverable (Low), Non-Critical (High), Critical (High) and Non-Recoverable (High)

The following information may appear for a selected sensor in the IPMI Numeric Sensors window, depending on whether the information is applicable to the sensor type:

- Lower Critical - Lower critical numeric sensor value.
- Lower Non-Critical - Lower non-critical numeric sensor value.
- Lower Non-Recoverable - Lower non-recoverable numeric sensor value.
- Negative Hysteresis - Negative hysteresis numeric sensor value.
- Positive Hysteresis - Positive hysteresis numeric sensor value.
- Upper Critical - Upper critical numeric sensor value.
- Upper Non-Critical - Upper non-critical numeric sensor value.
- Upper Non-Recoverable - Upper non-recoverable numeric sensor value.

The IPMI Numeric Sensor Details window may also contain one of three gauge types displaying the numeric sensor reading, including upper and lower thresholds and the status of the sensor. See *IPMI Viewer Window features* on page 230 for more information.

Customizing the IPMI Numeric Sensors window

By default, the following fields display in the IPMI Numeric Sensors window and may be removed using the *Customize* link:

- Name - The numeric sensor name. An icon representing the numeric sensor type will appear to the left of the name. Clicking on the name of the numeric sensor or its icon will display the IPMI Numeric Sensor Detail window.

  The name field also contains an icon that indicates the numeric sensor type (for example, fan, battery and so on) and may also contain an icon indicating whether the current value is within acceptable thresholds, as shown in Table 8.3.

Table 8.4: Numeric Sensor Threshold Icons

Icon	Description
None	The current value is within acceptable thresholds.
	(yellow circle) The current value is in the non-critical area.
	(red x) The current value is in the critical area.
	(dark red sad face) The current value is in the non-recoverable area.
	(question mark) The current value is unknown.

- Status - The numeric sensor status.
- Reading - The numeric sensor reading.
- Gauge - A graphic that displays the current numeric sensor reading and whether the reading is within a valid range. A pointer is positioned at the current reading. Depending on the numeric sensor, the gauge may contain any of the following items:
  - Green area - Normal values within the specified thresholds.
  - Yellow areas - Upper and lower non-critical threshold values.
  - Red areas - Upper and lower critical threshold values.
  - Dark red areas - Upper and lower non-recoverable threshold values.

  Figure 8.3 illustrates the gauge areas.

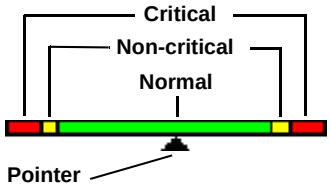


Figure 8.3: Numeric Sensor Threshold Gauge

NOTE: A gray gauge will appear if the numeric sensor values are invalid.

The following fields are not displayed by default, but may be displayed using the Customize link:

- Lower Critical - Lower critical numeric sensor value.
- Lower Non-Critical - Lower non-critical numeric sensor value.
- Lower Non-Recoverable - Lower non-recoverable numeric sensor value.
- Negative Hysteresis - Negative hysteresis numeric sensor value.
- Positive Hysteresis - Positive hysteresis numeric sensor value.
- Sensor Type - Numeric sensor type.
- Units - Numeric sensor units.
- Upper Critical - Upper critical numeric sensor value.
- Upper Non-Critical - Upper non-critical numeric sensor value.
- Upper Non-Recoverable - Upper non-recoverable numeric sensor value.

See *Using the Customize link in windows* on page 15 for more information.

To display IPMI target numeric sensor information:

1. From a Target Devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window, click on the name of a supported IPMI 1.5 target device. The side navigation bar will contain the name of the target device at the top and *Overview* will automatically be selected. The Unit Overview window will open.
2. Click *IPMI* in the side navigation bar, and then click *Numeric Sensors*. The IPMI Numeric Sensors window will appear.
3. Click on the name of a sensor. The IPMI Numeric Sensor window will open.
4. Click *Close* when you are finished to return to the IPMI Numeric Sensors window.
5. Click *Close* when you are finished to return to the Target Devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window.

Displaying the BMC system log and log events

The System Event Log window displays the BMC events which have occurred during the DSView software session.

If a user or a user group to which to a user belongs has Configure Unit Settings access rights for the IPMI 1.5 target device, the Clear Log button will appear in the System Event Log window. Clicking the *Clear Log* button clears all entries from the system event log on the IPMI 1.5 target device and writes the name of the IPMI 1.5 target device and the user who cleared the system event log to the event log. See *Changing Unit Access Rights* on page 102 for more information on setting access rights and *About Event Logs* on page 275 for more information.

The generated events will vary by BMC, motherboard and chassis implementation.

To display detailed information about a specific BMC event, click on the event name. The Event Entry Details window will open.

The following information appears in the Event Entry Details window about the selected sensor event:

- Sensor Name - Sensor name.
- Timestamp - Time, in the target device time zone, at which the event occurred on the IPMI 1.5 target device.

  If the BMC clock has not been synchronized with the PC clock, the timestamp may reflect the time relative to the startup of the host instead of the event occurrence.
- ID - Unique system event log (SEL) identifier used for retrieving events.
- Event Type - Event type.
- Sensor Type - Sensor type.
- Description - Description of the event.

Additional information provided by certain sensor events may also appear in the Event Entry Details window.

Customizing the System Event Log window

The Sensor Name and ID fields are always displayed in the System Event Log window.

By default, the Time, Description and Event Type fields display in the System Event Log window and may be removed using the Customize link:

The Sensor Type field is not displayed by default, but may be displayed using the Customize link:

See *Using the Customize link in windows* on page 15 for more information.

To display the BMC system log and log events:

1. From a Target Devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window, click on the name of a supported IPMI 1.5 target device. The side navigation bar will contain the name of the target device at the top and *Overview* will automatically be selected. The Unit Overview window will open.
2. Click *IPMI* in the side navigation bar, and then click *SEL*. The System Event Log window will open.
3. Click on the name of a sensor event name. The Event Entry Details window will open.
4. Click *Close* when you are finished to return to the System Event Log window.

5. Click Close when you are finished to return to the Target Devices, Units in Site, Units in Custom Field, Topology or Recently Accessed Units window.

CHAPTER 9

Using Tools

The DSView management software contains tools that may be used to perform various actions on managed appliances and target devices.

This chapter describes the available tools and how to use them. It also explains how to set up and use tasks in the DSView software.

Using Unit Tools

The Unit tools window contains tools that allow a user to:

- Export unit information into a .csv (comma separated value) file
- Export the access rights information for units in to .csv file
- Merge two or more target devices into a single target device
- Import a DSView 2.x software database into the DSView management software (valid only when the DSView software is installed on supported Windows systems)

To display the Units Tools window:

1. Click *Units* in the tab bar. *Units* will automatically be selected in the top navigation bar and a list of links will appear in the side navigation bar.
2. Click *Tools* in the side navigation bar. The Units Tools window will open.

Exporting units

The Export Units tool will export information about units into a .csv file with the default name unitproperties.csv. You may change the name of the file when it is saved.

The following unit information may be selected for export:

Name	Primary contact
Action (default action)	Primary contact phone
Browser URL	Secondary contact
Custom field 1-3	Secondary contact phone
Department	Serial number
DSView server name	Site

IP address	Status (at time of export)
Location	Telnet port
Model number	Type
Part number	Visibility (show or hide)

The output .csv file may be viewed in a text editor or spreadsheet application, such as Microsoft Excel.

To export units:

1. In the Units Tools window, click the *Export Units* icon or link. The Export Units Wizard will appear. Click *Next*.
2. The Select Unit Properties to Export window will open.
3. Specify the properties you wish to export:
   a. Select the properties in the Available Properties list. Multiple properties may be selected by pressing **Ctrl** or **Shift** while clicking on the property names.
   b. Click *Add*. The properties will be moved to the Properties to Export list.

      To remove selected properties, select the property you wish to remove from the Properties to Export list (multiple properties may be selected by pressing **Ctrl** while clicking on the property names) and clicking *Remove*. The properties will be moved to the Available Properties list.
   c. To change the order in which properties are listed in the output .csv file, select the properties in the Properties to Export list and use the up and down arrows to move the selected properties up or down in the listing. Multiple properties may be selected by pressing **Ctrl** or **Shift** while clicking on the property names.
   d. Click *Next*.
4. The Save Process window will open. Click *Next*.
5. The Completed Successful window will open, along with a File Download dialog box.

   Click *Open*. The file will download and open. By default, .csv files are configured to open in Microsoft Excel. If Microsoft Excel is not installed on your computer, you will be prompted to select a text editor to use for opening the .csv file.

NOTE: The default filename of the .csv file is unitproperties.csv. Subsequent files that you export will be incremented (unitproperties[1].csv, unitproperties[2].csv and so on).

   -or-

   Click *Save*. The Save As dialog box will appear. Select a directory and filename and click *Save* to save the .csv file.

   -or-

   Click *Cancel* to cancel the action.
6. Click *Finish*. The Units Tools window will open.

Exporting unit rights

The Export Unit Rights tool will export permission information about units from the DSView management software host. Managed appliance information will be exported into a .csv file with the default name appliance_rights.csv. Target device information will be exported into a .csv file with the default name target_device_rights.csv. You may change the names of the files when they are saved.

The following information will be exported for managed appliances:

- Appliance - The name of the managed appliance.
- User/User Group - The user or user group to which the managed appliance has any or all rights for the unit.
- Reboot - Whether the user or user group may reboot the managed appliance.
- Flash Upgrade - Whether the user or user group may Flash upgrade the managed appliance.
- Settings - Whether the user or user group may configure appliance settings, not including the right to manage local user accounts on the appliance.
- Local Users - Whether the user or user group may manage local users on the managed appliance.

The following information will be exported for target devices:

- Target Device - Name of the target device.
- User/User Group - User or user group to which managed appliances have any or all rights for the target device.
- Viewer Sessions - Whether the user or user group may launch a KVM or serial session with the target device.
- Power Control - Whether the user or user group may perform power control operations on the target device.
- VM Sessions - Whether the user or user group may launch a virtual media session with the target device.
- Reserved VM Sessions - Whether the user or user group may launch a reserved virtual media session with the target device.

The output .csv file may be viewed in a text editor or spreadsheet application, such as Microsoft Excel.

To export unit rights:

1. In the Units Tools window, click the *Export Unit Rights* icon or link. The Export Unit Rights Wizard will appear. Click *Next*.
2. The Select Unit Type window will open.
   a. Select *Appliances* to export the rights for managed appliances in your DSView software system.

      -or-

Select *Target Devices* to export the rights for target devices in your DSView software system.

b. Click *Next*.

3. The Save Process window will open. Click *Next*.
4. The Completed Successful window will open, along with a File Download dialog box.
5. Click *Open*. The file will download and open. By default, .csv files are configured to open in Microsoft Excel. If Microsoft Excel is not installed on your computer, you will be prompted to select a text editor to use for opening the .csv file.

NOTE: The default filename of the .csv file is appliance_rights.csv if you are exporting DS1800 digital switch, DSI5100, CPS and CCM appliance and DSR switch rights or target_device_rights.csv if you are exporting target device rights. Subsequent files that you export will be incremented (target_device_rights[1].csv, target_device_rights[2].csv and so on).

-or-

Click *Save*. The Save As dialog box will appear. Select a directory and filename and click *Save* to save the .csv file.

-or-

Click *Cancel* to cancel the action.

6. Click *Finish*. The Units Tools window will open.

Merging target devices

Using the Merge Target Devices tool may be necessary if a target device is connected to one or more managed appliances. For example, if a target device is connected to both a DSR switch and a CCM appliance, this tool will merge the target devices created when the managed appliances were added into a single target device that contains all of the target actions.

To merge target devices:

1. In the Units Tools window, click the *Merge Target Devices* icon or link. The Merge Target Devices Wizard will appear. Click *Next*.
2. The Select Target Devices to Merge window will open.
3. Specify the target devices you wish to merge:
   a. Select the target devices in the Available Target Devices list. Multiple target devices may be selected by pressing **Ctrl** or **Shift** while clicking on the target device names.
   b. Click *Add*. The target devices will be moved to the Target Devices to Merge list.

      To remove selected target devices from the Target Devices to Merge list, select the target device you wish to remove from the Target Devices to Merge list (multiple target devices may be selected by pressing **Ctrl** or **Shift** while clicking on the Target Device names) and clicking *Remove*. The target devices will be moved to the Available Target Devices list.
   c. To merge target devices in a particular order, select the target devices in the Target Devices to Merge list and use the up and down arrows to move the selected target devices

up or down in the listing. Multiple target devices may be selected by pressing **Ctrl** or **Shift** while clicking on the target device names. Once the order has been specified, select *Merge missing properties to the target device based on the order of the devices in the "Target Devices to Merge" list*.

The merged target devices will contain the name of the first target device in the Target Device to Merge list. For example, if you are merging two target devices named TD1 and TD2, and TD2 is listed before TD1, the merged target device will be named TD2.

d. Click *Next*.

4. The Confirm Target Device Merge window will open. Click *Next* to confirm merging the connection paths into the specified destination target device. See *Managing Connections to Units* on page 132 for more information.
5. The Completed Successful window will open.
6. Click *Finish*. The Units Tools window will open.

Importing DSView 2.x software databases

NOTE: This procedure is supported only when the DSView software is installed on a supported Windows system.

The Import DSView 2.x software database tool allows you to import an existing DSView 2.x software database into the DSView software system. When a database is imported, the following items will be imported:

- Units, including attached cascade switches, SPC devices and target devices
- Users and user groups with unit access rights
- Authentication services, including Windows NT domains, LDAP and local accounts
- System settings, including the ability to display connected users, connection sharing, status polling and delay rates and when the event log is deleted

The following actions occur when a DSView 2.x software database is imported into the DSView software system:

- A global unit group is created in the system for each group found in the DSView 2.x software database. The DSView management software does not provide DSView 2.x software Topology unit group nesting. Unit group names added to the system are a concatenation of the hierarchical names found in the DSView 2.x software, including the truncation of names when necessary.
- If a user had "admin" rights in the DSView 2.x software for all nodes in the tree (including the Topology node), the user will be added as a member and inherit the access rights of a DSView software administrator user group member in the DSView management software.

  If a user had "admin" rights in the DSView 2.x software for all nodes in the tree except for the Topology node, the user will be added as a member and inherit the access rights of an appliance administrator user group member in the DSView management software.

If a user had any other type rights in the DSView 2.x software, the user will be added as a member of the user group in the DSView management software. Access rights are set for units to which the user has access as follows:

- A user with “user” rights to a target device in the DSView 2.x software will be assigned the Establish Viewer Sessions access right in the DSView management software.
- A user with “admin” rights to a target device in the DSView 2.x software will be assigned the Configure Unit Settings, Establish Viewer Sessions and Control Target Device Power access rights in the DSView management software.
- A user with “user” rights to a DS1800 digital switch, CPS appliance or DSR switch in the DSView 2.x software will not be assigned any access rights in the DSView software.
- A user with “admin” rights to a DS1800 digital switch, CPS appliance or DSR switch in the DSView 2.x software will be assigned the Reboot Appliance, Flash Upgrade Appliance and Configure Appliance Settings access rights in the DSView software.

- Cascade switch types in the DSView 2.x software database cannot be determined during the import process and are added as Generic 1 x <n> switches, based on the number of found switch channels. After importing the DSView 2.x software database and running the Migrate DSView 2.X Units task, you may run the Resync Wizard on individual CPS appliances, DS1800 digital switches and DSR switches to specify switch types and merge multiuser switches. See *Resynchronizing managed appliances* on page 252 for more information.
- Internal users and built-in user groups with DSView 2.x software permissions residing on the computer that ran the DSAuth server will be imported into your DSView software system. An external NT authentication service with the same name as the DSAuth server will be added to the DSView software system. The DSView 2.x software users and user groups will be associated with the authentication service added to the DSView software system.
- The DSView 2.x software Everyone user group cannot be imported into DSView software systems.

Before using the Import DSView 2.x Software Database tool

To use the Import DSView 2.x Software Database tool, you must create a backup of the database using the DSAuth Migration Utility. The database is saved as a .zip file which may then be imported into the DSView software system using the Import DSView 2.x Database tool.

NOTE: The DSAuth Migration Utility will shut down the DSView 2.x DSAuth service as it runs and will restart the service upon completion.

1. On the computer containing the DSView 2.x software database (that is, the DSAuth Server) that you wish to migrate, Insert the DSView 3 Software CD. An autorun file will display the DSView management software screen.
2. Click *Run DSView 2.x Migration.*

   -or-

   If autorun is not enabled, type **<drive:>\Migration Utility\DSMigration.exe**, where <drive:> is the letter of your CD-ROM drive. The DSAuth Migration Utility dialog box will appear.

3. Click *Backup*. The Save As dialog box will appear.
4. Select a directory and filename and click *Save* to save the DSView 2.x software database backup. The Status area of the DSAuth Migration Utility dialog box will contain messages about the DSView 2.x software database backup as it is created. A Finished message box will appear when the backup is completed.
5. Click *OK* in the Finished message box.

To import DSView 2.x software databases:

1. In the Units Tools window, click the *Import DSView 2.x Database* icon or link. The Import DSView 2.x Database Wizard will appear.
   a. Use the *Browse* button to locate the .zip backup file of the DSView 2.x software database that you created.
   b. Click *Next*.
2. The Select Import Options window will open.
   a. Select *Import DSView 2.x system settings and apply them to this system* to allow the following settings to be imported from the DSView 2.x software database migration file into your DSView software system:
      - Whether connected users may be viewed. See *Specifying Video Viewer Session Settings* on page 177 for more information.
      - Whether connections are automatically shared when a KVM session is started. See *Specifying Video Viewer Session Settings* on page 177 for more information.
      - Whether polling is enabled or disabled. See *To use unit status polling* on page 84 for more information.
      - The delay between polling cycles. See *To use unit status polling* on page 84 for more information.
      - The retention time of the event log. See *Retaining the Event Log* on page 285 for more information.
   b. Select *Allow Target Devices to be added for nodes that have a default name* to allow target devices to be added to your DSView software system for nodes in the DSView 2.x software migration file that have default names. In DSView 2.x software, a default name is considered to be a name such as Port 1, Channel 1 and Socket 1.

      All default names are adjusted when they are imported to include the name of each CPS appliance, DS1800 digital switch and DSR switch.
   c. Select *Allow nodes with the same name to be merged into the same target device* if you wish to merge a target device that has multiple connections into a single target device. For example, a target device may be connected to a both a DSR switch and an SPC device.
   d. Select *Add Active Directory authentication services instead of NT authentication services when Active Directory is detected* to add an Active Directory service when an Active Directory domain is detected in the DSView 2.x software database migration file. If this

option is not selected, the service will be added to the DSView software system as a Windows NT Domain service.

e. Type the case-insensitive names of any DSView 2.x software database nodes that you do not wish to import, separated by commas (,), in the *Node Names to Ignore* field. Any children within the parent nodes listed in the field are also ignored (that is, not imported).

   You may import a node containing a comma on its name by enclosing the node name within quotation marks. For example, to import a node named node, two (containing a comma) and a node named nodeone, type ”node,two”,nodeone in the Node Names to Ignore field.

f. Click *Next*.

3. The Import in Progress window will open, updating to show the current step being performed, as the DSView 2.x software database is importing. The Completed Successful window will open when the import has completed and will contain a summary of the import, including the following information:
   - Number of authentication services added
   - Number of users added
   - Number of user groups added
   - Number of units added
   - Number of unit groups added
4. Click *Finish*. The Units Tools window will open.

After running the Import DSView 2.x Database tool

The Migration Status field is enabled and displays in Unit Views windows. Units requiring migration will contain Migration Needed in the Migration Status field.

Although the DS1800 digital switches, CPS appliances and DSR switches have been imported from the DSView 2.x software database into the DSView software system, they are not yet compatible with the DSView management software. To complete the configuration and update the firmware on each type of DS1800 digital switch, CPS appliance and DSR switch, you must use the Migrate Units task. See *Task: Migrating DSView 2.x units to DSView software compatible units* on page 264 for more information.

Using the Managed Appliance Tools

The DSView management software contains tools that allow you to perform the following actions on a DS1800 digital switch, DSI5100, CPS or CCM appliance or DSR switch:

- Reboot
- Upgrade the firmware
- Resynchronize the managed appliance so that it reflects the current DSView software system configuration

The following actions may be performed on a DS1800 digital switch, CPS appliance, CCM appliance or DSR switch:

- Save or restore the configuration
- Save or restore the database of local users

These tools are accessed from the Unit Overview window, which is displayed when you click on the name of the managed appliance.

To access the managed appliance tools:

1. Click *Units* in the tab bar. *Units* will automatically be selected in the top navigation bar and a list of links will appear in the side navigation bar.
2. In the side navigation bar, do one of the following:
   - Click *Appliances*. The Appliances - All window will open. You may also click on a link below Appliances to display only specific types of DS1800 digital switches, DSR switches, CPS appliances or CCM appliances in an Appliances window.
   - Click *Topology*. The Topology window will open.
   - Click *Sites* and then click on a site link. A Units in Site window will open.
   - Click a custom field label and then the appropriate label that you specified for the managed appliance. The Units in Custom Fields window will open.
   - If the managed appliance has been recently accessed, click *Recently Accessed* to display the Recently Accessed Units window.
3. Click on the name of a managed appliance. *Overview* will automatically be selected in the side navigation bar and the Unit Overview window will open. The tools will appear in the Tools area of the window.

Rebooting

To reboot a managed appliance:

NOTE: To reboot a DSR switch, CPS appliance or CCM appliance, you must have Reboot Appliance access rights. By default, users who are members of the DSView software administrators, user administrators and appliance administrators built-in groups have this access right. See *Changing Unit Access Rights* on page 102 for more information.

1. In the Unit Overview window, click the *Reboot* icon or link. A confirmation dialog box will appear.
2. Click *Yes* to confirm or *No* to cancel. If confirmed, all active sessions will be disconnected.

Upgrading firmware

To upgrade the firmware on a managed appliance:

NOTE: A valid Flash file must exist in the DSView software server's firmware repository for the DS1800 digital switch, DSI5100, CPS or CCM appliance or DSR switch to use this command. Optionally, one or more managed appliances may be Flash upgraded as a task. See *Managing Tasks* on page 255 for more information.

1. In the Unit Overview window, click the *Upgrade Firmware* icon or link. The Upgrade Appliance Firmware Wizard will appear. Click *Next*.
2. The Select Firmware Files window will open. Select the Flash files to which you wish to upgrade the managed appliance:
   a. Select the Flash files in the Available Firmware Files list. Multiple firmware files may be selected by pressing **Ctrl** or **Shift** while clicking on the firmware filenames.
   b. Click *Add*. The properties will be moved to the Firmware Files to Update list.

      To remove selected firmware files, select the firmware file you wish to remove from the Firmware Files to Update list (multiple firmware files may be selected by pressing **Ctrl** or **Shift** while clicking on the firmware filenames) and clicking *Remove*. The firmware files will be moved to the Available Firmware Files list.
   c. To change the order in which firmware files are installed on the managed appliance, select the firmware files in the Firmware Files to Update list and use the up and down arrows to move the selected firmware files up or down in the listing. Multiple firmware files may be selected by pressing **Ctrl** or **Shift** while clicking on the firmware filenames.
   d. Click *Next*.

      When multiple firmware files are selected, the firmware on each managed appliance will be upgraded in the order shown in the Update list. A reboot will be automatically performed between each firmware update.
3. The Type in Task Name window will open. Type a name for the upgrade firmware task (1-64 characters), then click *Next*.
4. The Completed Successful window will open.
5. Click *Finish*. The Unit Overview window will open.
6. The progress of the upgrade task can be checked by clicking the *System* tab and then clicking *Tasks* in the top navigation bar.

Resynchronizing managed appliances

When a DS1800 digital switch, DSI5100, CPS or CCM appliance or DSR switch changes its configuration, it may not be properly represented in the DSView software system. For example, a target device may be added, removed or moved. Resynchronizing will update these and other changes made to the managed appliance within the DSView software system.

Resynchronizing will force a check of the entire DSView software system. The process requires a large amount of time and network bandwidth and should only be performed when necessary.

To resync a managed appliance:

1. In the Unit Overview window, click the *Resync* icon or link. The Resync Appliance Wizard will appear. Click *Next*.
2. The Select Resync Options window will open.
   a. Click *Allow existing target devices to be renamed* to allow target devices to be renamed in the DSView software with target device name changes in the managed appliance.
   b. Click *Allow target devices that contain default names to be added* to allow target devices that have default names in the managed appliances to be added to the DSView software database.
   c. Click *Allow target devices with the same name to be merged into a single target device* to allow the DSView software to treat multiple target devices with the same name as one unit with multiple access methods.
   d. Click *Remove offline connections* to remove any connections to target devices that are offline from the DSView software system.
   e. Click *Next*.
3. If the managed appliance does not require resynchronizing, the Completed Successful window will appear.

   -or-

   If the managed appliance requires resynchronizing, the Changes Detected in Appliance window will open. Click *Next* and go to step 7.

   -or-

   If one or more cascade switches are attached to the DS1800 digital switch or DSR switch, the Cascade Switch Configuration window will open. Continue to step 4.
4. From the drop-down menu, select the type of each detected cascade switch.
5. Type a name for each cascade switch.
6. If you wish, combine any multiuser cascade switches. Click the checkboxes of the cascade switches that you wish to merge, and then click *Merge*.

   To unmerge any cascade switches that you have merged, click the checkbox of the merged cascade switch and then click *Split*.
7. Click *Next*. The Completed Successful window will open.
8. Click *Finish*. The Unit Overview window will open.

Saving a managed appliance configuration

You may save the configuration of a DS1800 digital switch, CPS appliance, CCM appliance or DSR switch to a file. The configuration file will contain information about the managed appliance, including the following:

- Global settings
- Port settings

- SNMP trap settings
- SNMP manager settings
- The names of connected target devices

For information on restoring a configuration file, see *Restoring a managed appliance configuration* on page 254.

To save a managed appliance configuration to a file:

1. In the Unit Overview window, click the *Save Configuration* icon or link. The Save Appliance Configuration Wizard will appear. Click *Next*.
2. The Type in File Description window will open. Type a description of the configuration that will be saved and may be used if you wish to restore the configuration at a later time, and then click *Next*.
3. The Completed Successful window will open.
4. Click *Finish*. The Unit Overview window will open.

Restoring a managed appliance configuration

You may restore the configuration of a DSR switch, CPS appliance or CCM appliance. To restore the configuration, a previously-saved configuration file must exist. See *Saving a managed appliance configuration* on page 253 for more information.

Appliance Configuration files are stored in the DSView software server appliance files repository. You may display the available configuration files by selecting the *System* tab, selecting *Appliance Files* in the top navigation bar and selecting *Configuration* in the side navigation bar.

NOTE: The managed appliance must be rebooted to enable the restored configuration file.

To restore a managed appliance configuration:

1. In the Unit Overview window, click the *Restore Configuration* icon or link. The Restore Appliance Configuration Wizard will appear. Click *Next*.
2. The Select Configuration to Restore window will open. Click the radio button to the left of the file containing the configuration you wish to restore, and then click *Next*.
3. The Completed Successful window will open.
4. Click *Finish*. The Unit Overview window will open.
5. Reboot the managed appliance to enable the configuration. See *Rebooting* on page 251 for more information.

Saving the user database of a managed appliance

NOTE: You may not save the user database of a DS1800 digital switch or DSR1161, DSR2161, DSR4160, DSR800 switch.

You may save the local user database on a DSR switch (except as noted above), CPS appliance or CCM appliance. For information on restoring a user database, see *Restoring the user database of a managed appliance* on page 255.

To save the user database of a managed appliance:

1. In the Unit Overview window, click the *Save User Database* icon or link. The Save Appliance User Database Wizard will appear. Click *Next*.
2. The Type in File Description window will open. Type a description of the user database that will be saved and can be used if you wish to restore the database, and then click *Next*.
3. The Completed Successful window will open.
4. Click *Finish*. The Unit Overview window will open.

Restoring the user database of a managed appliance

NOTE: You may not restore the user database of a DS1800 digital switch or DSR1161, DSR2161, DSR4160, DSR800 switch.

You may restore the local user database of a DSR switch, CPS appliance or CCM appliance. To restore the user database, a previously saved user database file must exist. See *Saving the user database of a managed appliance* on page 254 for more information.

Database files are stored in the DSView software server appliance files repository. You may display the available database files by selecting the *System* tab, selecting *Appliance Files* in the top navigation bar and selecting *User Database* in the side navigation bar.

NOTE: The managed appliance must be rebooted to enable the restored user database file.

To restore the user database of a managed appliance:

1. In the Unit Overview window, click the *Restore User Database* icon or link. The Restore Appliance User Database Wizard will appear. Click *Next*.
2. The Select User Database to Restore window will open. Click the radio button to the left of the managed appliance user database you wish to restore, and then click *Next*.
3. The Completed Successful window will open.
4. Click *Finish*. The Unit Overview window will open.
5. Reboot the managed appliance to enable the user database. See *Rebooting* on page 251 for more information.

Managing Tasks

The Tasks window allows you to add, delete and change tasks. The Tasks window lists all existing tasks configured in the DSView management software and allows you to manually run tasks.

To display the Tasks window:

1. Click the *System* tab.
2. Click *Tasks* in the top navigation bar. The Tasks window will open.

Customizing the Tasks window

By default, the following fields display in the Tasks window:

NOTE: The Next Run and Last Run fields will be blank for a task scheduled on a remote DSView software server.

- Runs On - Displays the server(s) on which the task will run.
- Next Run - Displays the next date and time on which the task is scheduled to run.
- Last Run - Displays the date and time of the last run of the task.
- Status - The status of a task. An icon will also appear in the Name column that represents the status of the task.

  Table 9.1 describes the status icons that may appear in the Tasks window.

Table 9.1: Task Status Icons

Icon	Task
	Idle - A task that is not currently running
	Running - A task that is currently occurring
	Stopping - A task that has run but not completely stopped
	Disabled - A task that is prevented from executing
	Remote - A task that is scheduled on a remote DSView software server

The Schedule field (how often and when the task is scheduled to run) may be displayed in the Tasks window by clicking the *Customize* link. See *Using the Customize link in windows* on page 15 for more information.

Adding tasks

You may use the Add Task Wizard to run the following tasks:

- Backup the DSView software database and system files

- Configure SNMP trap settings on appliance
- Control power of target devices
- Export event log to comma separated values (.csv) file
- Migrate units (configures and upgrades DSView 2.x or AVWorks software units)

  DSView 2.x software units may only be migrated when the DSView 3 software is installed on a supported Windows system
- Send IPMI chassis control command to target devices
- Upgrade firmware of selected appliances of the same type
- Validate external authentication server user accounts

Specifying when to run tasks

You may choose to run tasks at the following times:

- Run task now - Choosing this option will run the task immediately after you click *Finish* when adding the task in the Add Task Wizard. The Status column will indicate Running and the running icon will appear to the left of the task name.
- One time only - Choosing this option will run the task once at a specific time on a specific date.
- Periodic - Choosing this option will run the task a certain number of times per hour or day, beginning at a specific time on a specific date.
- Daily - Choosing this option will run the task once every day, once Monday-Friday or regularly for a certain number of days (every 2 days, every 3 days and so on), beginning at a specific time on a specific date.
- Weekly - Choosing this option will run the task once each week or regularly over a certain number of weeks (every 2 weeks, every 3 weeks and so on), beginning at a specific time on a specific date. You may also specify which days you wish for the task to run.
- Monthly - Choosing this option will run the task once each month or regularly over a certain number of months (every 2 months, every 3 months and so on) beginning at a specific time on a specific date. You may also specify which months you wish for the task to run.

To run a task periodically:

1. In the Select When to Run the Task window, click *Periodic*. Click *Next*.
2. The Specify Periodic Schedule window will open.
   a. Select the hour, minute and AM or PM from the drop-down menus to select the time to begin running the task.
   b. Click *Every (minutes)* and select a number of minutes from the drop-down menu.

      -or-

      Click *Every (hours)* and select a number of hours from the drop-down menu.
   c. Click on the calendar button or the field to the left of the calendar button and select a date to begin running the task. To use the calendar:

- Click on the year and select a year from the drop-down menu that will appear.
- Click on the month name and select a month from the drop-down menu that will appear.

  -or-

  Use the arrows at the top of the calendar to move forward and backward by month.
- Click on a day in the calendar to close the calendar and fill the field to the left of the calendar with the date you have selected.

To run a task daily:

1. In the Select When to Run the Task window, click *Daily.* Click *Next*.
2. The Specify Daily Schedule window will open.
   a. Select the hour, minute and AM or PM from the drop-down menus to select the time to begin running the task.
   b. Click *Every Day* to run the task each day of the week (Sunday-Saturday).

      -or-

      Click *Weekdays* to run the task once each weekday (Monday-Friday).

      -or-

      Click *Every (days)* and select the number of consecutive days (1-365) from the drop-down menu.
   c. Click on the calendar button or the field to the left of the calendar button and select a date to begin running the task. To use the calendar:
      - Click on the year and select a year from the drop-down menu that will appear.
      - Click on the month name and select a month from the drop-down menu that will appear.

      -or-

      Use the arrows at the top of the calendar to move forward and backward by month.
      - Click on a day in the calendar to close the calendar and fill the field to the left of the calendar with the date you have selected.

To run a task weekly:

1. In the Select When to Run the Task window, click *Weekly,* then click *Next*.
2. The Specify Weekly Schedule window will open.
   a. Select the hour, minute and AM or PM from the drop-down menus to select the time to begin running the task.
   b. Click *Every (weeks)* and select the number of consecutive weeks (1-52) from the drop-down menu.
   c. Select the day of week to run the task from the list box. Multiple days may be selected by pressing **Ctrl** while clicking on the days.

d. Click on the calendar button or the field to the left of the calendar button and select a date to begin running the task. To use the calendar:
   - Click on the year and select a year from the drop-down menu.
   - Click on the month name and select a month from the drop-down menu.

     -or-

     Use the arrows at the top of the calendar to move forward and backward by month.
   - Click on a day in the calendar. The calendar will close and fill the field to the left of the calendar with the selected date.

To run a task monthly:

1. In the Select When to Run the Task window, click *Monthly.* Click *Next*.
2. The Specify Monthly Schedule window will open.
   a. Select the hour, minute and AM or PM from the drop-down menus to select the time to begin running the task.
   b. Click *Day* and select the day of the month to run the task using the drop-down menu.

      -or-

      Click *The* and select a week and a day of the week to run the task using the drop-down menus. For example, if you wish to run the task each second Tuesday of the month, select *second* from the first drop-down menu and *Tuesday* from the second drop-down menu.
   c. Select the month to run the task from the list box. Multiple months may be selected by pressing **Ctrl** while clicking on the days.
   d. Click on the calendar button or the field to the left of the calendar button and select a date to begin running the task. To use the calendar:
      - Click on the year and select a year from the drop-down menu.
      - Click on the month name and select a month from the drop-down menu or use the arrows at the top of the calendar to move forward and backward by month.
      - Click on a day in the calendar. The calendar will close and fill the field to the left of the calendar with the selected date.

Adding tasks using the Add Task Wizard

Tasks may only be added by DSView software administrators.

Task: Backup DSView database and system files

This task creates a compressed .zip file containing a backup of your DSView software system. The backup file contains everything necessary to fully restore the DSView software hub server. The backup file is named dsviewBackup.zip by default, but you may also append the date and time to the end of the backup filename.

If a backup is restored to a server with a different IP address, managed appliances may not be able to authenticate until the new DSView software server IP address has been programmed into the managed appliances.

To add the task:

1. In the Tasks window, click *Add*. The Add Task Wizard will appear. Click *Next*.
2. The Select Task to Add window will open.
   a. Select *Backup DSView database and system files* from the drop-down menu.
   b. Type a 1-64 character name for the task.
   c. Click *Next*.
3. The Select When to Run the Task window will open. Select a time to run the task, and then click *Next*. See *Specifying when to run tasks* on page 257 for more information.
4. The Specify DSView System Backup Properties dialog box will appear.
   a. Type the directory location in which to create the system backup, which may be a local drive on the DSView software server or at a network location specified by a UNC path.

      The directory name must be entered in case sensitive text if your operating system supports case sensitive filenames.
   b. Click *Login required to access shared drive location* if the location specified is a network path that requires a log in. Then, type the username and password and confirm the password of a user account that has read/write access to the network share location.

      The Location field cannot be set to a mapped network drive. It must be set to either a physical local drive or a shared network location specified as a UNC (Universal Naming Convention) path.
   c. Click *Encrypt Backup File* to encrypt the created system backup file and type a password used to lock and unlock the encrypted file.
   d. Click *Use date and time for file naming* to append the date and time (in military time) to the end of the system backup filename. For example, if you are creating the backup file on October 1, 2004 at 10:04 pm, the file created will be named dsviewBackup1001042204.zip.

      If a system backup file already exists in the specified directory and this option is not used, the existing backup file will be overwritten when the new backup file is created.
5. The Completed Successful window will open. Click *Finish*. The Tasks window will open including the new task.

Task: Configure SNMP trap settings on a managed appliance

This task turns SNMP traps on or off for one or more managed appliances of a particular type. To specify SNMP trap settings for other types of managed appliances, you must create additional tasks.

To add the task:

1. In the Tasks window, click *Add*. The Add Task Wizard will appear. Click *Next*.

2. The Select Task to Add window will open.
   a. Select *Configure SNMP trap settings on appliance* from the drop-down menu.
   b. Type a 1-64 character name for the task.
   c. Click *Next*.
3. The Select When to Run the Task window will open. Select a time to run the task (see *Specifying when to run tasks* on page 257 for more information), then click *Next*.
4. The Select Unit Group window will open. Select *All Appliances* or select a unit group, then click *Next*.
5. The Select Appliance Type window will open. Select the type of managed appliance for which to configure SNMP traps, then click *Next*.
6. The Select Appliances window will open. Depending on the selections made in step 4, the Available Appliances list will contain all managed appliances available from the unit group specified or all managed appliances.
   a. Select the managed appliance. Multiple managed appliances may be selected by pressing **Ctrl** or **Shift** while clicking on the managed appliance names.
   b. Click *Add*. The unit(s) will be moved to the Appliances to Configure list.
   c. Click *Next*.
7. The Configure SNMP Traps window will open.
   a. Change the state of each SNMP trap by selecting on of the following from each trap's drop-down menu:
      - *No Change* - leaves the trap on/off state to the state already configured.
      - *Enable* - turns the trap on.
      - *Disable* - turns the trap off.

      -or-

      Click one of the following buttons:
      - *No Change All* - uses the on/off states already configured.
      - *Enable All* - turns all traps on.
      - *Disable All* - turns all traps off.
   b. Click *Next*.
8. The Completed Successful window will open. Click *Finish*. The Tasks window will open, including the new task.

Task: Power control a target device

This task powers up, powers down or cycles the power (power down and then power up) of one or more target devices.

To add the task:

1. In the Tasks window, click *Add*. The Add Task Wizard will appear. Click *Next*.

2. The Select Task to Add window will open.
   a. Select *Control power of Target Devices* from the drop-down menu.
   b. Type a 1-64 character name for the task.
   c. Click *Next*.
3. The Select When to Run the Task window will open. Select a time to run the task (see *Specifying when to run tasks* on page 257 for more information), then click *Next*.
4. The Select Unit Group window will open.
   a. Select *All Target Devices* from the drop-down menu to configure the power control settings on all target devices.

      -or-

      Select a particular unit group to configure from the drop-down menu. See *Grouping units by unit group* on page 141 for more information.
   b. Click *Next*.
5. The Select Target Devices window will open. The Available Target Devices list will contain all target devices available in the unit group specified in the previous step.
   a. Select the target device from the Available Target Devices list. Multiple target devices may be selected by pressing **Ctrl** or **Shift** while clicking on the target device names.
   b. Click *Add*. The target device(s) will be moved to the Target Devices to Control list.
   c. Click *Next*.
6. The Select Power Control Function window will open.
   a. Select the power control function to be performed on the target devices:
      - *Turn Power On* - powers up the specified target devices.
      - *Turn Power Off* - powers down the specified target devices.
      - *Cycle Power* - powers down and then power up the specified target devices.
   b. Click *Next*.
7. The Completed Successful window will open. Click *Finish*. The Tasks window will open including the new task.

Task: Exporting an event log .csv file

This task exports selected fields from the DSView software system event log to a .csv file. The exported event log may be stored on a local or network drive. The event log is named eventlog.csv by default, but you may also append the date and time to the end of the event log. The output .csv file may be viewed in a text editor or spreadsheet application, such as Microsoft Excel.

You may also save an event log using the Export Event Log tool. See *Using the Event Log Tool* on page 288 for more information.

To add the task:

1. In the Tasks window, click *Add*. The Add Task Wizard will appear. Click *Next*.

2. The Select Task to Add window will open.
   a. Select *Export event log to a comma separated values (.CSV) file* from the drop-down menu.
   b. Type a 1-64 character name for the task.
   c. Click *Next*.
3. The Select When to Run the Task window will open. Select a time to run the task (see *Specifying when to run tasks* on page 257 for more information), then click *Next*.
4. The Specify Export Event Log Properties window will open.
   a. Type the directory in which to create the event log, which may be a local drive on the DSView software server or at a location specified by a UNC path. The directory name must be entered in case sensitive text if your operating system supports case sensitive filenames.
   b. Click *Login required to access shared drive location* if the location specified is a network drive that requires a log in. Then, type the username and password and confirm the password of a user account that has read/write access to the network share location. The Location field cannot be set to a mapped network drive. It must be set to either a physical local drive or a shared network location specified as a UNC path.
   c. Click *Use date and time for file naming* to append the date and time (in military time) to the end of the event log file. For example, if you are creating the event log file on October 1, 2004 at 10:04 pm, the file created will be named eventlog1001042204.csv.

      If an event log exists in the specified directory and you do not use this option, it will be overwritten when the new event log is created.
   d. Click *Next*.
5. The Select Event Log Columns to Export window will open. Add or remove the columns of information that you wish to export. See *Customizing the Event Log window* on page 276 for more information.

   To add a column of information:

   - Select the column to export from the Available Columns list. Multiple columns may be selected by pressing **Ctrl** or **Shift** while clicking on the column names.
   - Click *Add*. The column(s) will be moved to the Columns to Export list.

   To remove a column of information:

   - Select the column to remove from the Columns to Export list. Multiple columns may be selected by pressing **Ctrl** or **Shift** while clicking on the column names.
   - Click *Remove*. The column(s) will be moved to the Available Columns list.

   To change the order in which exported columns are listed in the output .csv file, select the columns in the Columns to Export list and use the up and down arrows to move the selected columns up or down in the listing. Multiple columns may be selected by pressing **Ctrl** while clicking on the column names.

e. Click *Next*.

6. The Completed Successful window will open. Click *Finish*. The Tasks window will open, including the new task.

Task: Migrating DSView 2.x units to DSView software compatible units

NOTE: This task is valid only when the DSView 3 software is installed on a supported Windows system.

This task updates DS1800 digital switches, CPS appliances or DSR switches within the unit group, or any of those managed appliances using firmware compatible with DSView 2.x software to firmware that is compatible with the DSView management software.

The managed appliances should not be Flash upgraded from DSView 2.x firmware to firmware that supports DSView 3 software before using the Migrate Units command. The recommended procedure is to first import the DSView 2.x software database to the new DSView software system using the Import DSView 2.x Database tool (see *Importing DSView 2.x software databases* on page 247), followed by running the Migrate Units task on each managed appliance.

A CPS appliance or DSR switch that has been migrated to DSView 3 software compatible firmware may be returned to DSView 2.x compatibility.

To add the task:

1. In the Tasks window, click *Add*. The Add Task Wizard will appear. Click *Next*.
2. The Select Task to Add window will open.
   a. Select *Migrate Units* from the drop-down menu.
   b. Type a 1-64 character name for the task.
   c. Click *Next*.
3. The Select When to Run the Task window will open. Select a time to run the task (see *Specifying when to run tasks* on page 257 for more information), then click *Next*.
4. The Select Unit Group window will open.
   a. Select *Units Needing Migration* from the drop-down menu.

      -or-

      Select a particular unit group from the drop-down menu.
   b. Click *Next*.
5. The Select Appliance Type window will open. Select the type of managed appliance to migrate, and then click *Next*. You must create a separate task for each type of DS1800 digital switch, CPS appliance or DSR switch you wish to migrate. For example, if you wish to migrate DSR1021, DSR2010 and DSR2010 switches and CPS1610 appliances, you must create four Migrate Units tasks.
6. The Select Appliances window will open. The Available Appliances list will contain only units with a status or Migration Needed that match the selected type found in the unit group specified in the previous step. Select the specific DS1800 digital switch, CPS appliance or

DSR switch to migrate from the Available Appliances list, and then click *Next*. Multiple switches or appliances may be selected by pressing **Ctrl** while clicking on the managed appliance names. Click *Add*. The switches or appliances will be moved to the Appliances to Configure list.

7. The Select Options for Migration window will open.
   a. Select *Enable secure mode* if you wish for all DS1800 digital switches, CPS appliances or DSR switches you are migrating to only be accessible by this DSView software system.

      -or-

      Uncheck *Enable secure mode* if you wish for all DS1800 digital switches, CPS appliances or DSR switches you are migrating to be accessible by any DSView software system.
   b. Click *Next*.
8. The Select Firmware Files for Migration window will open.
   a. Type the host name or the address of the TFTP server, in standard dot notation (xxx.xxx.xxx.xxx) containing the DS1800 digital switch, CPS appliance or DSR switch firmware files required for migration to DSView management software compatibility.
   b. Type the name of each firmware image.
   c. Click *Next*.
9. The Completed Successful window will open. Click *Finish*. The Tasks window will open including the new task.

   You may display the current progress of the migration task by clicking on the name of the task in the Tasks window.
10. Repeat steps 1-9 for each type of DS1800 digital switch, CPS appliance and DSR switch that you wish to migrate.

    Units successfully migrated into your DSView software system will appear in Unit Views windows and the Migration Status field for these units will contain Migration Completed. (Migration Needed appears for units requiring migration.)

Task: Migrating AVWorks software CCM appliances to DSView software compatible units

This task updates any CCM appliances within the unit group, or any CCM appliances using firmware compatible with the AVWorks software to firmware that is compatible with the DSView software.

Before an AVWorks software CCM appliance can be migrated, you must ensure that it is Flashed with bootstrap and application images at version 2.2 or higher. This procedure is described in the CCM Appliance Migration document, which is available on the Avocent web site.

The AVWorks software CCM appliance must be added to the DSView software system before it is migrated (see *Adding Units* on page 88). When you add the appliance, you will be alerted that it must be migrated, along with a link named Add Migration Task, which will take you to the Add Task Wizard.

A CCM appliance that has been migrated to DSView management software compatible firmware may be returned to AVWorks software compatibility. See the CCM Installer/User Guide for more information.

To add the task:

1. In the Tasks window, click *Add*. The Add Task Wizard will appear. Click *Next*.
2. The Select Task to Add window will open.
   a. Select *Migrate Units* from the drop-down menu.
   b. Type a 1-64 character name for the task.
   c. Click *Next*.
3. The Select When to Run the Task window will open. Select a time to run the task (see *Specifying when to run tasks* on page 257 for more information), then click *Next*.
4. The Select Unit Group window will open.
   a. Select *Units Needing Migration* from the drop-down menu.

      -or-

      Select a particular unit group from the drop-down menu.
   b. Click *Next*.
5. The Select Appliance Type window will open.

   Select the type of CCM appliance to migrate: CCM850, 1650 or 4850, and then click *Next*.

   You must create a separate task for each type of CCM appliance you wish to migrate. For example, if you wish to migrate CCM850, 1650 and 4850 appliances, you must create three Migrate Units tasks.
6. The Select Appliances window will open. The Available Appliances list will contain only units with a status or Migration Needed that match the selected type found in the unit group specified in the previous step.
   a. Select the specific CCM appliance to migrate. Multiple appliances may be selected by pressing **Ctrl** while clicking on the managed appliance names.
   b. Click *Add*. The appliances will be moved to the Appliances to Configure list.
   c. Click *Next*.
7. The Select Options for Migration window will open.
   a. Select *Enable secure mode* if you wish for all the CCM appliances you are migrating to only be accessible by this DSView software system.

      -or-

      Uncheck *Enable secure mode* if you wish for all CCM appliances you are migrating to be accessible by any DSView software system.
   b. Select *Enable target devices that contain default names to be added* if you wish to add them to the DSView software system.

-or-

Uncheck *Enable target devices that contain default names to be added* to exclude them.

c. Select *Allow target devices with the same name to be merged into a single target device* if you wish to have them merged.

-or-

Uncheck *Allow target devices with the same name to be merged into a single target device* if you do not wish to have them merged.

d. Click *Next*.

8. The Select Firmware Files for Migration window will open. Select the file image in the Available Firmware Files list, then click *Add*. The selected file will be moved to the Firmware File To Update list. Click *Next*.

   If needed, the firmware file may be added to the DSView software system from the Appliance Firmware Files window (accessed by selecting the *System* tab, *Appliance Files* in the top navigation bar, and *Firmware Files* in the side navigation bar).

9. The Enter in Login Credentials window will open.
   a. In the Username field, enter a 3-16 character username. This username must be the same for all CCM appliances selected for migration; otherwise, the appliance without this username will fail to migrate.
   b. The Password field is optional. If specified, the password must be 3-16 characters.
   c. Click *Next*.

10. The Completed Successful window will open. Click *Finish*. The Tasks window will open including the new task.

    You may display the current progress of the Migrate Units task as it is running using the Task Results window. To display the Task Results window, click on the name of the task in the Tasks window.

11. Repeat steps 1-9 for each type of CCM appliance that you wish to migrate.

Units successfully migrated into your DSView software system will appear in Unit Views windows and the Migration Status field for these units will contain Migration Complete.

Task: Sending an IPMI chassis control command to target devices

This command powers up, powers down, cycles the power (power down and then power up), performs a gentle shutdown or resets one or more IPMI 1.5 target devices.

You must have Control Target Device Power rights to send an IPMI chassis control command. See *Changing Unit Access Rights* on page 102 for more information.

To add the task:

1. In the Tasks window, click *Add*. The Add Task Wizard will appear. Click *Next*.
2. The Select Task to Add window will open.
   a. Select *Send IPMI chassis control command to target devices* from the drop-down menu.

b. Type a 1-64 character name for the task.

c. Click *Next*.

3. The Select When to Run the Task window will open. Select a time to run the task (see *Specifying when to run tasks* on page 257 for more information). Click *Next*.
4. The Select Unit Group window will open.
   a. Select *All Target Devices* from the drop-down menu to configure the IPMI chassis control on all target devices.

      -or-

      Select a particular unit group to configure from the drop-down menu. See *Grouping units by unit group* on page 141 for more information.

   b. Click *Next*.
5. The Select Target Devices window will open. The Available Target Devices list will contain all IPMI 1.5 target devices available in the unit group specified in the previous step.
   a. Select the specific IPMI 1.5 target devices to chassis control from the Available Target Devices list. Multiple target devices may be selected by pressing **Ctrl** or **Shift** while clicking on the target device names.
   b. Click *Add*. The IPMI 1.5 target devices will be moved to the Target Devices to Control list.
   c. Click *Next*.
6. The Select IPMI Control Function window will open.
   a. Select the power control function you wish to perform on the IPMI 1.5 target devices:
      - *Turn Power On* - powers up the specified devices.
      - *Turn Power Off* - powers down the specified devices.
      - *Cycle Power* - powers down and then power up the specified devices.
      - *Reset* - performs a hard reset of the specified devices.
      - *Graceful Shutdown* - performs a graceful shutdown of the specified devices.

NOTE: The availability of the Cycle Power and Graceful Shutdown options is dependent on the BMC implementation. If one of these options is selected for a task but the BMC implementation does not support the option, the task will fail when run and be reported in the Task Results window.

   b. Click *Next*.
7. The Completed Successful window will open. Click *Finish*. The Tasks window will open including the new task.

Task: Updating the firmware of an appliance type

This task upgrades the firmware of selected DS1800 digital switches, DSI5100, CPS or CCM appliances or DSR switches. To upgrade other types of managed appliances, you must create additional tasks.

Firmware must be available before using this command. See *Firmware Management* on page 272 for more information.

To add the task:

1. In the Tasks window, click *Add*. The Add Task Wizard will appear. Click *Next*.
2. The Select Task to Add window will open.
   a. Select *Update firmware of selected appliances of the same type* from the drop-down menu.
   b. Type a 1-64 character name for the task.
   c. Click *Next*.
3. The Select When to Run the Task window will open. Select a time to run the task (see *Specifying when to run tasks* on page 257 for more information), and then click *Next*.
4. The Select Unit Group window will open.
   a. Select *All Appliances* from the drop-down menu to upgrade all units.

      -or-

      Select a particular unit group to upgrade from the drop-down menu. See *Grouping units by unit group* on page 141 for more information.
   b. Click *Next*.
5. The Select Appliance Type window will open. Select the type of managed appliance that you wish to upgrade, and then click *Next*.
6. The Select Appliances list will contain all switches and appliances available in the unit group specified in the previous step.
   a. Select the specific managed appliance that you wish to upgrade from the Available Appliances list. Multiple switches or appliances may be selected by pressing **Ctrl** or **Shift** while clicking on the managed appliance names.
   b. Click *Add*. The unit(s) will be moved to the Appliances to Configure list.
   c. Click *Next*.
7. The Completed Successful window will open. Click *Finish*. The Tasks window will open, including the new task.

Task: Validating user accounts on an external authentication server

This task may be used to ensure that LDAP and Active Directory external authentication services contain accounts for users. Any user accounts not found on the external authentication server will be flagged as suspicious (a question mark icon will appear to the left of the user's name). Suspicious accounts are indicated in event log files.

To add the task:

1. In the Tasks window, click *Add*. The Add Task Wizard will appear. Click *Next*.
2. The Select Task to Add window will open.

a. Select *Validate external authentication server user accounts* from the drop-down menu.
b. Type a 1-64 character name for the task.
c. Click *Next*.

3. The Select When to Run the Task window will open. Select a time to run the task (see *Specifying when to run tasks* on page 257 for more information), then click *Next*.
4. The Completed Successful window will open. Click *Finish*. The Tasks window will open, including the new task.

Running tasks manually

Although tasks are scheduled to run at particular times using the Add Task Wizard, you may run an existing task at any time you wish.

To manually run tasks:

1. In the Tasks window, click the checkbox to the left of the task(s) you wish to run.

   -or-

   Click the checkbox to the left of Name column at the top of the list to select all tasks listed in the window.

NOTE: Remote tasks that are scheduled on another DSView software Server, may not be run from the DSView software server to which you are logged in. To run a remote task, you must log in to the DSView software server on which the task was created.

2. Click *Run Now*. The icon to the left of the task name will change to the running icon and the status of the task will change to Running.

Displaying task results

The Task Results window displays the status of the most current run of tasks, including successful and unsuccessful runs and information on each run.

The following fields display in the Task Results window for the Configure SNMP trap settings on appliance, Control power of target devices, Migrate DSView 2.X Units, Send IPMI chassis control command to target devices and Upgrade firmware of selected appliances of the same type tasks:

- Name - Names of the DS1800 digital switch, DSI5100, CPS or CCM appliance, DSR switch or IPMI 1.5 target device on which the task is running or has been run
- Start Time - Exact time at which each task run occurred
- Duration - Date and time of the task run
- Status - Result of the task run

To display the results of a task:

From the Tasks window, click the name of the task for which you wish to display the results. *Results* will automatically be selected in the side navigation bar and the Task Results window will

display, containing information about the task run. The side navigation bar will include the name of the task that you are viewing.

Deleting tasks

NOTE: Remote tasks, which are scheduled on another DSView software server, may not be deleted from the DSView software server to which you are logged in. To delete a remote task, you must log in to the DSView software server on which the task was created.

To delete a task:

1. In the Tasks window, click the checkbox to the left of the task(s) you wish to delete.

   -or-

   Click the checkbox to the left of Name column at the top of the list to select all tasks listed in the window for deletion.
2. Click *Delete*. A confirmation dialog box will appear.
3. Click *OK* to confirm or *Cancel* to cancel.

Changing tasks

NOTE: Remote tasks, which are scheduled on another DSView software server, may not be modified from the DSView software server to which you are logged in. To change a remote task, you must log in to the DSView software server on which the task was created.

You may change the schedule and properties for existing tasks. (The Validate external authentication server user accounts task does not contain properties.)

To change a task schedule:

1. In the Tasks window, click the name of the task you wish to change. The side navigation bar will include the name of the task that you are changing.
2. Click *Schedule* in the side navigation bar. The Task Schedule window will open. Select the type of task you wish to schedule and complete the information. See *Specifying when to run tasks* on page 257 for more information.

To change the properties of a task:

1. In the Tasks window, click the name of the task you wish to change. The side navigation bar will include the name of the task that you are changing.
2. Click *Properties* in the side navigation bar. A Task Properties window will open.
3. Change the properties of the task. See the operating sequence for the task type in *Adding tasks using the Add Task Wizard* on page 259 for more information.

Firmware Management

The Flash firmware files for DS1800 digital switches, DSI5100, CPS and CCM appliances and DSR switches may be added, viewed and deleted using the Appliance Firmware Files window. Once a Flash firmware file(s) has been added, you may use the file(s) to upgrade the managed appliance.

To display the Appliance Firmware Files window:

1. Click the *System* tab.
2. Click *Appliance Files* in the top navigation bar. *Appliance Files - Firmware* will automatically be selected in the side navigation bar and the Appliance Firmware Files window will appear.

Customizing the Appliance Firmware Files window

By default, the following field displays in the Appliance Firmware Files window: version, firmware type, appliance type, creation date and time and description.

You may customize the Appliance Firmware Files window by adding language and country information. See *Using the Customize link in windows* on page 15 for more information.

To add a firmware file:

1. In the Appliance Firmware Files window, click *Add*. The Add Firmware File Wizard will appear. Click *Next*.
2. The Select Firmware File to Import window will open.
3. Enter the directory and filename of the firmware file you want to add to the DSView management software appliance files repository. Alternately, you may browse for the file by clicking the *Browse* button.
4. Type a description of the firmware file in the Description field.
5. Click *Next*. The firmware is added and the Completed Successful window appears.
6. Click *Finish*. The Appliance Firmware Files window will open including the added firmware file.

NOTE: Once the file is uploaded, it is no longer needed on the DSView software client from which it was uploaded.

To display firmware information:

1. In the Appliance Firmware Files window, click on the version of a firmware file. The Firmware File Properties window will open.
2. The display includes the firmware version, appliance type, firmware creation date, country and language of the firmware. If you wish, you may change the description of the firmware file in the Description field.
3. Click *Save* and then click *Close*. The Appliance Firmware - All window will open and contain the firmware information if you saved the changes.

To delete firmware:

1. In the Appliance Firmware Files window, select the checkbox(es) of any firmware you wish to delete.
2. Click the *Delete* button. A confirmation dialog box will appear.
3. Click *Yes* to confirm or *No* to cancel.

CHAPTER 10

Event Logs

Whenever a defined event occurs in the DSView management software system, it is saved in the event log. Examples of events that may be logged include changes in the state of a managed appliance, an unsuccessful login to the DSView management software, the completion of tasks and logouts.

This chapter describes how to manage event logs and how to configure email notifications when events occur.

About Event Logs

The types of event log entries are predefined in the DSView software. See *DSView management software events* on page 277 for more information.

To display event log entries, click *Reports* in the tab bar. *Event Log* will automatically be selected in the top navigation bar, *Event Log Views - All* will automatically be selected in the side navigation bar and the Event Log-All window will open. The Event Log - All window contains a listing of all event log events that have occurred on the DSView software system.

Non-recoverable, critical or non-critical events may be viewed by users who are members of the administrators or auditors user group by clicking one of the icons which appears in the top navigation bar of the DSView Explorer window. The number of the specific type of event appears to the right of the icon.

Event log data may be exported from the DSView software into a comma separated value (.csv) file. The .csv file may be viewed in a text editor or spreadsheet application, such as Microsoft Excel.

Users may specify how long event information is retained in the DSView software database by using the Event Log Retention Time window.

NOTE: Event log information is stored in the DSView software database and is replicated. Increasing the event log retention time may impact the performance of your DSView software system. It is recommended that old event log entries be archived to .csv files by scheduling tasks. See *Managing Tasks* on page 255 for more information.

Clicking on the following links beneath Event Log Views in the side navigation bar will expand the link and display additional sub-links:

- Severity Level - Displays links that may be clicked to display event log entries of a particular severity level (Monitor, Information, OK, Non-Critical, Critical or Non-Recoverable).
- Event Category - Displays links that may be clicked to display event log entries in a particular event category (System, Authentication, Users, Units, Tasks, Unit Status, Access Control or Sessions).

Clicking on a link beneath Severity Level or Event Category in the side navigation bar will display a window containing a listing of all event log events in the DSView software system that belong to that particular type.

Additional commands are available in the side navigation bar to disable currently enabled events, specify how long the event log should be retained, specify who should be notified by email when an event log event occurs and to export the event log to a .csv file.

Detailed information about an event log event may be viewed by clicking on its name in the Severity column.

Customizing the Event Log window

The following columns are always displayed in the Event Log window:

- Severity - Displays information about an event log entry. Clicking on an event log entry in this column will display the Event Log Event Information window, which contains detailed information about the entry. An icon will also appear to the left of the item name. Table 10.1 lists the icons that will appear for various severity levels.

Table 10.1: Event Log Severity Icons

Icon	Description
	Monitor event
	Information event
	OK event
	Non-critical event
	Critical event
	Non-recoverable event

- Date/Time - Displays the date and time of an event in the client computer’s time zone.

By default, the following column displays in an Event Log window and may be removed by clicking the *Customize* link:

- Description - Displays a short description of an event. See *DSView management software events* on page 277 more information.

By default, the following columns do not display in the Event Log window and may be added by clicking the *Customize* link:

- Category - Displays the category of an event log entry. Available categories include: Appliance, System, Authentication, Users, Units, Tasks, Unit Status, Access Control, Sessions and Target Device.
- Detailed Description - Displays detailed information about an event. Detailed descriptions may include items such as the name of a target device, session type (KVM, serial or virtual media), DSView software server, user and so on. For example, an MIB-II interface link up trap would contain *Appliance change of state* in the Description column, while the Detailed Description column would contain *Generic link up interface 1*.
- DSView Server - Displays the name of the DSView software server where the event was logged.
- Event ID - Displays a unique identifier for an event. The Event ID column is useful for filtering and sorting displays based on a specific event type.
- Trap Enterprise - Displays the enterprise object identifier for a received SNMP trap.
- Unit - Displays the name of a managed appliance for an event.
- User - Displays the user associated with an event. For example, this column shows the name of the user who deleted a unit when a Unit Deleted event is detected.

See *Using the Customize link in windows* on page 15 for more information.

DSView management software events

Table 10.2 lists the appliance events that may occur within a DSView software system.

Table 10.2: Appliance Events

Event ID	Description	Event ID	Description
1:0	An unrecognized event was received	1:11	Appliance upgrade result
1:1	Appliance cold start	1:12	Appliance authentication failure
1:2	Appliance warm start	1:13	Appliance diagnostic information
1:3	Appliance session started	1:14	Appliance user logged in
1:4	Appliance session stopped	1:15	Appliance user logged out
1:5	Appliance session terminated	1:16	Appliance alert from attached server
1:6	Appliance component added	1:17	Appliance configuration changed

Table 10.2: Appliance Events (Continued)

Event ID	Description	Event ID	Description
1:7	Appliance component removed	1:18	Appliance command issued
1:8	Appliance component restarted	1:19	Appliance incorrect state detected
1:9	Appliance change of state	1:20	Appliance threshold exceeded
1:10	Appliance upgrade started		

Table 10.3 lists the system events that may occur within a DSView software system.

Table 10.3: System Events

Event ID	Description	Event ID	Description
2:1	DSView software server <server name> started successfully	2:66	DSView software server added
2:2	DSView software server <server name> started with errors	2:80	Too many SNMP traps are being received
2:3	The <server name> service failed to start	2:81	Too many SNMP traps were received
2:4	DSView software server <server name> stopped	2:96	Backup server <server name> successfully registered
2:16	Too many events are being received	2:97	Backup server <server name> registration failed
2:17	Too many events were received	2:98	DSView software server <server name> is now configured as a primary server
2:32	System disabled due to a license violation (duplicate key)	2:99	DSView software server <server name> failed to become a primary server
2:33	A license violation was detected (duplicate key)	2:100	Server <server name> failed to register with the new primary
2:34	A client license violation was detected (first warning)	2:112	Due to naming conflicts <device names> were renamed
2:35	A client license violation was detected (second warning)	2:115	A database snapshot of the hub was required
2:36	A client license violation was detected (third warning)	2:128	Database backup successful

Table 10.3: System Events (Continued)

Event ID	Description	Event ID	Description
2:37	A client license violation was detected (final)	2:129	Database backup failed, {0}
2:48	SSL server certificate updated	2:130	Database restore successful
2:64	DSView software server configuration was updated	2:131	Database restore failed
2:65	DSView software server deleted		

Table 10.4 lists the authentication events that may occur within a DSView software system.

Table 10.4: Authentication Events

Event ID	Description	Event ID	Description
3:1	Authentication successful	3:6	Authentication server added
3:2	Logout successful	3:7	Authentication server modified
3:3	Authentication failure	3:8	Authentication server deleted
3:4	External authentication server authentication failed	3:16	LDAP search returned bad continuation reference
3:5	Server authentication failure		

Table 10.5 lists the user and user group events that may occur within a DSView software system.

Table 10.5: User and User Group Events

Event ID	Description	Event ID	Description
4:1	User account locked	4:5	User account deleted
4:2	User account unlocked	4:6	User group added
4:3	User account added	4:7	User group modified
4:4	User account modified	4:8	User group deleted

Table 10.6 lists the unit events that may occur within a DSView software system.

Table 10.6: Unit Events

Event ID	Description	Event ID	Description
5:1	Unit group added	5:19	Unit custom fields modified

Table 10.6: Unit Events (Continued)

Event ID	Description	Event ID	Description
5:2	Unit group deleted	5:20	Target devices merged
5:3	Unit group modified	5:21	Appliance configuration file added
5:4	Site added	5:22	Appliance configuration file modified
5:5	Site modified	5:23	Application configuration file deleted
5:6	Site deleted	5:24	User database file added
5:7	Location added	5:25	User database file modified
5:8	Location modified	5:26	User database file deleted
5:9	Location deleted	5:28	Power on command issued
5:10	Department added	5:29	Power off command issued
5:11	Department modified	5:30	Power cycle command issued for <device>
5:12	Department deleted	5:31	Unit <unit name> rebooted
5:13	Firmware file added	5:32	Unit reset
5:14	Firmware file modified	5:33	Unit identity light turned on
5:15	Firmware file deleted	5:34	Unit gracefully powered off
5:16	Unit added	5:35	System event log (SEL) cleared
5:17	Unit modified	5:36	Unit identity light turned off
5:18	Unit deleted		

Table 10.7 lists the task events that may occur within a DSView software system.

Table 10.7: Task Events

Event ID	Description	Event ID	Description
6:1	Task started	6:6	Task added
6:2	Task completed successfully	6:7	Task modified
6:3	Task started manually	6:8	Task deleted
6:4	Scheduled task failed	6:9	Task failed
6:5	Scheduled task failed		

Table 10.8 lists the unit status events that may occur within a DSView software system.

Table 10.8: Unit Status Events

Event ID	Description	Event ID	Description
7:1	Loss of communication	7:2	Regained communication (RCM)

Table 10.9 lists the access control events that may occur within a DSView software system.

Table 10.9: Access Control Events

Event ID	Description	Event ID	Description
8:1	Access rights modified		

Table 10.10 lists the session events that may occur within a DSView software system.

Table 10.10: Session Events

Event ID	Description	Event ID	Description
9:1	Session started	9:11	Global modified
9:2	Session stopped	9:12	Global macro deleted
9:3	Session terminated	9:20	Global macro group added
9:4	Session preempted	9:21	Global macro group modified
9:10	Global macro group added	9:22	Global macro group deleted

Displaying Event Logs

NOTE: The 5000 most recent log events may be viewed in one of the Event Log windows using the side navigation bar links. To use the side navigation bar links to display older events in Event Log windows, you must use the date filter. See *Using the Date Filter* on page 283 for more information.

To display a specific type of event log entry using the side navigation bar:

From the side navigation bar under Event Log Views, click *All* to display a list of all available event logs. The Event Log - All window will open.

-or-

Click *Severity Level* to display a list of event log entries that match a given severity level and then click on one of the following:

- *Monitor* - Displays the Event Log - Monitor Events window, which displays events that are periodic and expected.

- *Information* - Displays the Event Log - Information Events window, which displays events that are neither periodic nor problematic.
- *OK* - Displays the Event Log - OK Level Events window, which displays events that are in a normal or cleared state. This value typically appears at event start up or after leaving a previous event state.
- *Non-Critical* - Displays the Event Log - Non-Critical Events window, which displays abnormal events that require correcting at a later time.
- *Critical* - Displays the Event Log - Critical Events window, which displays abnormal events of a more serious nature that may require quicker action, such as the failure of a scheduled task or loss of communication.
- *Non-Recoverable* - Displays the Event Log - Non-Recoverable Events window, which displays severe abnormal events impacting your DSView management software session and requires immediate corrective action.

-or-

Click *Event Category* to display a list of event logs belonging to a specific category in the side navigation bar and then click on one of the following:

- *Appliance* - Displays the Event Log - Appliance Events window, which displays events related to managed appliances.
- *System* - Displays the Event Log - System Events window, which displays events related to the DSView management software host server, global settings, licenses, tasks or firmware.
- *Authentication* - Displays the Event Log - Authentication Events window, which displays events related to user login and authentication.
- *Users* - Displays the Event Log - User Events window, which displays events relating to users.
- *Units* - Displays the Event Log - Unit Events window, which displays events related to units (managed appliances and target devices), unit groups, sites, departments or locations.
- *Tasks* - Displays the Event Log - Task Events window, which displays events related to the starting or stopping of an event.
- *Unit Status* - Displays the Event Log - Unit Status Events window, which displays events related to the loss of or regaining of communication with a managed appliance.
- *Access Control* - Displays the Event Log - Access Control Events window, which displays events related to a user's privileges for working with specific managed appliances.
- Sessions - Displays the Event Log - Session Events window, which displays events related to serial, KVM and virtual media sessions.

See *DSView management software events* on page 277 for more information.

To display non-recoverable, critical or non-critical event log entries using the top navigation bar:

NOTE: Only members of the Administrator or Auditor user groups may display these event log entries.

Click one of the icons in table Table 10.11 to display the specific type of event.

Table 10.11: Top Navigation Bar Event Log Icons

Icon	Description
	This icon indicates non-recoverable events. Clicking it displays the Event Log - Non-Recoverable Events window.
	This icon indicates critical events. Clicking it displays the Event Log - Critical Events window.
	This icon indicates non-critical events. Clicking it displays the Event Log - Non-Critical Events window.

Using the Date Filter

When viewing event log entries, an additional filter is available that allows you to display either all events of a particular type or a series of events between two specific periods.

The event log retains all events occurring in the DSView software system for the specified retention time. The 5000 most recent events may be displayed using the side navigation bar links beneath the Event Log Views heading in an unfiltered Event Log window. To use the side navigation bar links to display older events in an Event Log window, you may specify a range for when the events you wish to display occurred. The older events will then appear in Event Log windows when you select the side navigation bar links.

To display all events of a particular type:

1. In an Event Log window, click *Date Filter*. The Date Filter window will open.
2. In the first drop-down menu in the From line, select *First Event*.
3. In the first drop-down menu in the To line, select *Last Event*.
4. Click *Apply*. The previous event log view window will open including all events.

To display event log entries between two specific periods using the date filter:

1. In an Event Log window, click *Date Filter*. The Date Filter window will open.
2. In the first drop-down menu in the From line, select *Events On* to pick the start date and time for event log entries you wish to view.
3. Click on the calendar button or the field to the left of the calendar button and select a start date. To use the calendar:
   a. Click on the year and select a year from the drop-down menu that will appear.
   b. Click on the month name and select a month from the drop-down menu that will appear.

      -or-

      Use the arrows at the top of the calendar to move forward and backward by month.

c. Click on a day in the calendar to close the calendar and fill the field to the left of the calendar with the date you have selected.

4. Select an hour, minute and which half of the day for the start date.
5. In the first drop-down menu in the To line, select *Events On* to pick the end date and time for event log entries you wish to view.
6. Repeat steps 3 and 4 to specify the end date period.
7. Click *Apply.* The previous event log view window will open with the event range specified in the Filter Date window. The Clear Date Filter button will appear in the event log view window. Clicking the button will display all events available for the event type and the button will no longer be available in the window.

Displaying the Details of Event Log Entries

You may display all logged information about a specific event log entry.

To display the details of an entry in the event log:

1. In an Event Log window, click on the link in the Severity column for which you wish to display details. The Event Information window will open and contain information about the event log entry.

NOTE: Trap Enterprise in the Event Log-All window is named Enterprise OID in the Event Information window.

2. Click *Close*. The Event Log window will open.

Deleting Event Log Entries

To delete an entry from the event log:

1. In an Event Log window, click the checkbox to the left of the event(s) you wish to delete.

   -or-

   Click the checkbox to the left of Severity at the top of the list to select all events listed in the window for deletion.
2. Click *Delete*. A confirmation dialog box will appear.
3. Click *OK* to delete the event(s).

   -or-

   Click *Cancel* to cancel the action.

Enabling and Disabling Events

Events occurring on your DSView software system may be disabled using the Enabled Log Events window. When an event is disabled, its state will appear as *Disabled* and the event will not be logged until it is reenabled. An event may be reenabled by selecting it and clicking *Enable*.

You may change the number of items that display in the Enabled Log Events window by clicking the *Customize* link. See *Using the Customize link in windows* on page 15 for more information.

To enable or disable an event in the event log:

1. Click *Enabled Events* in the side navigation bar. The Enabled Log Events window will open and display a listing of all enabled and disabled log events.
2. Click the checkbox to the left of an enabled event you wish to disable or a disabled event you wish to enable.

   -or-

   Click the checkbox to the left of Log Event at the top of the list to select all events listed in the window.

NOTE: Events may not be enabled unless they are already disabled.

3. Click *Enable* to enable the selected events.

   -or-

   Click *Disable* to disable the selected events.

   The Enabled Log Events window will re-appear including the updated status of the listed events.

Retaining the Event Log

By default, an event log is retained for one week. However, you may specify a retention time of up to one year.

Event log information is stored in the DSView software database and is replicated. Increasing the event log retention time may impact the performance of your DSView software system. It is recommended that old event log entries be archived to .csv files by scheduling tasks. See *Managing Tasks* on page 255 for more information.

To specify an event log retention time:

1. Click *Log Retention* in the side navigation bar. The Event Log Retention Time window will appear.
2. Type a number of days (from 1-365) in the Days field, or select it using the drop-down menu.
3. Click *Save* to save your changes.

Configuring Email Notifications

NOTE: The Simple Mail Transfer Protocol (SMTP) must be configured to receive email notifications about events.

The DSView management software may be configured to send one or more users email notifications when events occur. Multiple events may be configured so that an email is sent to the

defined users any time one of the specified events occurs. See *DSView management software events* on page 277 more information.

Customizing the Email Notifications window

The Email Subject column is always displayed in the Email Notifications window: You may add the From Address and To Address, using the Customize link. See *Using the Customize link in windows* on page 15 for more information.

To configure an email notification:

1. Click *Email Notifications* in the side navigation bar. The Email Notifications window will appear.
2. Click *Add*. The Add Email Notification Wizard will appear. Click *Next*.
3. The Specify Email Properties window will open.
   a. Type the names of all individuals that you wish to receive a notification in the Send To field. Multiple users may be added by separating each email address with a comma (,).

      The Send To field has a maximum limit of 1024 characters.

   b. Type the email address of the person you wish to designate as the sender of the notification in the From field.

      The From field has a maximum limit of 64 characters.

   c. Type a subject heading for the notification in the Subject field.

      The Subject field has a maximum limit of 64 characters.

   d. Click *Next*.
4. The Select Events to Trigger Email Notification window will open.
   a. Add or remove events that will cause an email to be sent to the specified individuals.

      To add an event:

      - Select the event you wish to add to the notification from the Available Events list. Multiple events may be selected by pressing **Ctrl** while clicking on the event names.
      - Click *Add*. The event(s) will be moved to the Events To Notify list.

      To remove an event already assigned to the notification:

      - Select the event you wish to remove from the Events To Notify list. Multiple events may be selected by pressing **Ctrl** while clicking on the event names.
      - Click *Remove*. The events will be moved to the Available Events list.

   b. Click *Next*.
5. The Completed Successful window will open. Click *Finish*.

Changing email notifications

To change an email notification:

1. Click *Email Notifications* in the side navigation bar. The Email Notifications window will appear.
2. Click on the email subject of the notification you wish to change. The Email Notification Properties window will appear.
3. Change the notification:
   a. Type the names of (or remove) any individuals that you wish to receive the notification in the Send To field. Multiple users may be added by separating each email address with a comma (,). The Send To field has a limit of 1024 characters.
   b. Change the email address of the person you wish to designate as the sender of the notification in the From field. The From field has a limit of 64 characters.
   c. Change the subject heading for the notification in the Subject field. The Subject field has a limit of 64 characters.
   d. Add or remove events that will cause an email to be sent to the specified individual(s). See *DSView management software events* on page 277 for more information.

      To add an event:

      - Select the event you wish to add to the notification from the Available Events list. Multiple events may be selected by pressing **Ctrl** while clicking on the event names.
      - Click *Add*. The events will be moved to the Events To Notify list.

      To remove an event already assigned to the notification:

      - Select the event you wish to remove from the Events To Notify list. Multiple events may be selected by pressing **Ctrl** while clicking on the event names.
      - Click *Remove*. The events will be moved to the Available Events list.
4. Click *Save* and then click *Close*. The Email Notifications window will open including the renamed notification.

Deleting email notifications

To delete an email notification:

1. Click *Email Notifications* in the side navigation bar. The Email Notifications window will appear.
2. Click the checkbox to the left of the notifications you wish to delete.

   -or-

   Click the checkbox to the left of Email Subject at the top of the list to select all notifications listed in the window for deletion.
3. Click *Delete*. A confirmation dialog box will appear.
4. Click *OK* to confirm or *Cancel* to cancel.

Testing email notifications

Once an email notification has been created, you may send a test message to ensure that the notification is delivered to the specified recipients.

To test an email notification:

1. Click *Email Notifications* in the side navigation bar. The Email Notifications window will appear.
2. Click the checkbox to the left of the notification(s) you wish to test.

   -or-

   Click the checkbox to the left of Email Subject at the top of the list to select all notifications listed in the window for testing.
3. Click *Test*. A confirmation dialog box will appear.
4. Click *OK* to confirm or *Cancel* to cancel the action.

Using the Event Log Tool

All or selected columns of the event log can be exported as a comma separated values (.csv) file. The output event log file is named eventlog.csv by default, but you may change the name when it is saved.

The fields that may be exported correspond with those that appear in the Event Log windows. See *Customizing the Event Log window* on page 276 for more information.

The .csv file may be viewed in a text editor or spreadsheet application, such as Microsoft Excel.

NOTE: The event log may also be exported to a .csv file by creating a task. See *Managing Tasks* on page 255 for more information.

To create an event log .csv file:

1. Click *Tools* in the side navigation bar. The Event Log Tools window will open.
2. Click the *Export Event Log* icon or text. The Export Event Log Wizard will appear.
3. Click *Next*.
4. The Select Columns to Export window will open.
5. Add or remove the columns of information that you wish to export.

   To add a column of information:

   a. Select the column you wish to export from the Available Columns list. Multiple columns may be selected by pressing **Ctrl** while clicking on the column names.

   b. Click *Add*. The columns will be moved to the Columns to Export list.

   To remove a column of information:

   a. Select the column you wish to remove from the Columns to Export list. Multiple columns may be selected by pressing **Ctrl** while clicking on the column names.

b. Click *Remove*. The columns will be moved to the Available Columns list.

6. To change the order in which exported columns are listed in the output .csv file, select the columns in the Columns to Export list and use the up and down arrows to move the selected columns up or down in the listing. Multiple columns may be selected by pressing **Ctrl** while clicking on the column names.
7. Click *Next*.
8. The Save Process window will open explaining how the file will be saved. Click *Next*.
9. The Completed Successful window will open, along with a File Download dialog box.
10. From the File Download dialog box, click *Open*. The file will be downloaded and will open on the DSView software client. By default, .csv files are configured to open in Microsoft Excel. If Microsoft Excel is not installed on your computer, you will be prompted to select a text editor to open the .csv file.

    -or-

    From the File Download dialog box, click *Save*. The Save As dialog box will appear. Select a directory and filename and click *Save* to save the .csv file.

    -or-

    Click *Cancel* to cancel the action.
11. Click Finish. The Event Log Tools window will open.

APPENDICES

Appendix A: Technical Support

Our Technical Support staff is ready to assist you with any installation or operating issues you encounter with your Avocent product. If an issue should develop, follow the steps below for the fastest possible service:

1. Check the pertinent section of the manual to see if the issue may be resolved by following the procedures outlined.
2. Check our web site at www.avocent.com/support to search the knowledge base or use the on-line service request.
3. Call the Avocent Technical Support location nearest you.

Appendix B: TCP and UDP Ports

The DSView software client accesses the server and performs commands using a standard web browser. The communication protocol used between the client web browser and the server is the HTTPS protocol. By default, TCP/IP port 443 is used for HTTPS connections, but you may change the port using the DSView Server Network Properties window.

NOTE: The port used for the HTTPS connection may be changed using the DSView Server Network Properties window. The HTTPS port must be specified in the web browser URL if changed from the default (port 443). See *Server Properties* on page 49 for more information.

DSView software clients may communicate with the DSView software server through a standard connection or using a proxy server. By default, TCP/IP port 1078 is used for proxied connections. If a proxy connection has not been created, TCP ports 22, 2068 and 8192 must be configured as open on your firewall.

DS1800 digital switch and DSR switch ports

A user may initiate a KVM session with a target device on a DS1800 digital switch or DSR switch by clicking *KVM Session* for the appropriate target device or by clicking the *KVM Session* icon or text from a Unit Overview window.

The client contacts the DSView software server, which checks the permissions of the target device. If the logged in user has permissions to establish Video Viewer sessions to the selected target device, the server will establish a connection to the DS1800 digital switch or DSR switch using TCP/IP port 3871 to authorize the session. The KVM data is sent to the DS1800 digital switch or DSR switch using ports 8192 and 3871. Port 8192 contains the video portion of the KVM data. Port 2068 contains the keyboard and mouse portion of the KVM data.

In a non-proxied connection, the video data from port 8192 and the keyboard and mouse data from port 2068 are sent directly from the client to the DS1800 digital switch or DSR switch. Figure B.1 illustrates the ports used with a non-proxied DS1800 digital switch or DSR switch connection.

UDP port 3211 is used by the DSView software server to initialize the IP configuration of DS1800 digital switches and DSR switches. TCP/IP port 3211 is also used by the DSView software server to perform management functions on DS1800 digital switches and DSR switches, such as configuring settings.

NOTE: When using a non-proxied connection, video performance over a slower network connection may be less than optimal. Since certain color settings (such as grayscale) use less network bandwidth than others (such as Best Color), changing the color settings may increase video performance. For optimal video performance over a slower network connection, a color setting such as grayscale/Best Compression or Low Color/High Compression is recommended. See *Adjusting color depth* on page 181 for more information.

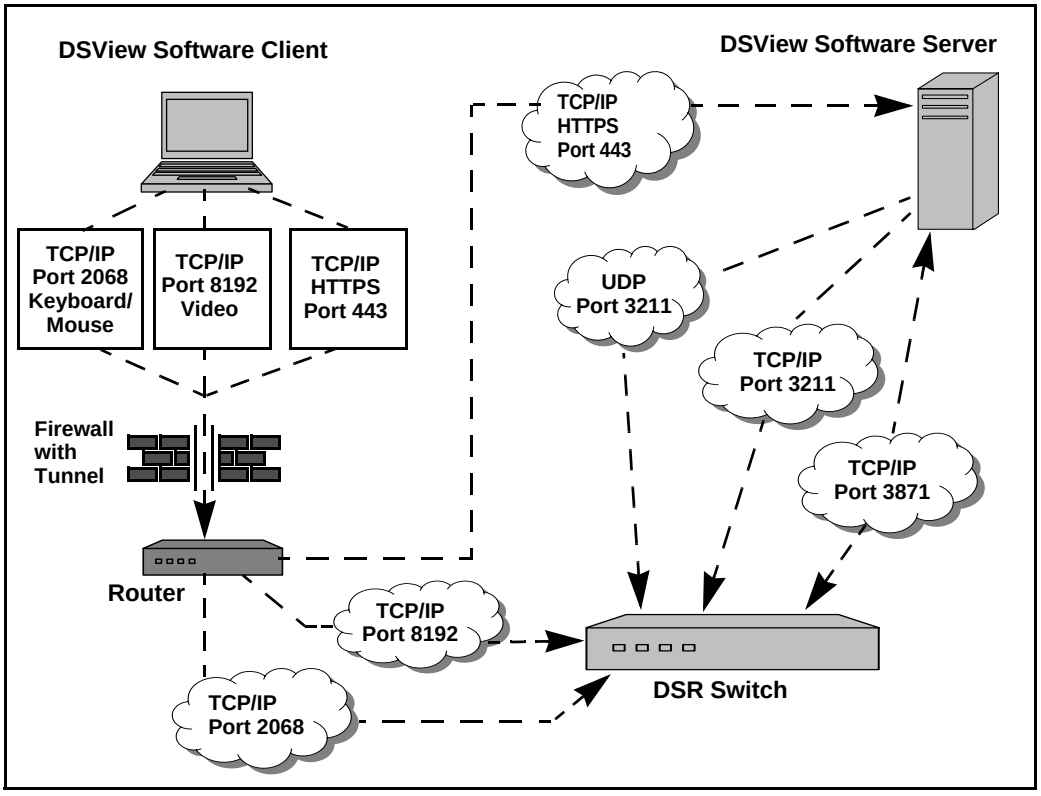


Figure B.1: Ports Used with a DS1800 Digital Switch or DSR Switch Connection (KVM) Without Proxy

In a proxied connection, communication with TCP/IP ports 8192 and 2068 occurs between the server and the DS1800 digital switch or DSR switch instead of directly between the client and the DS1800 digital switch or DSR switch. The client receives information by communicating back and forth with the server using port 1078. Figure B.2 illustrates the ports used with a proxied DS1800 digital switch or DSR switch connection.

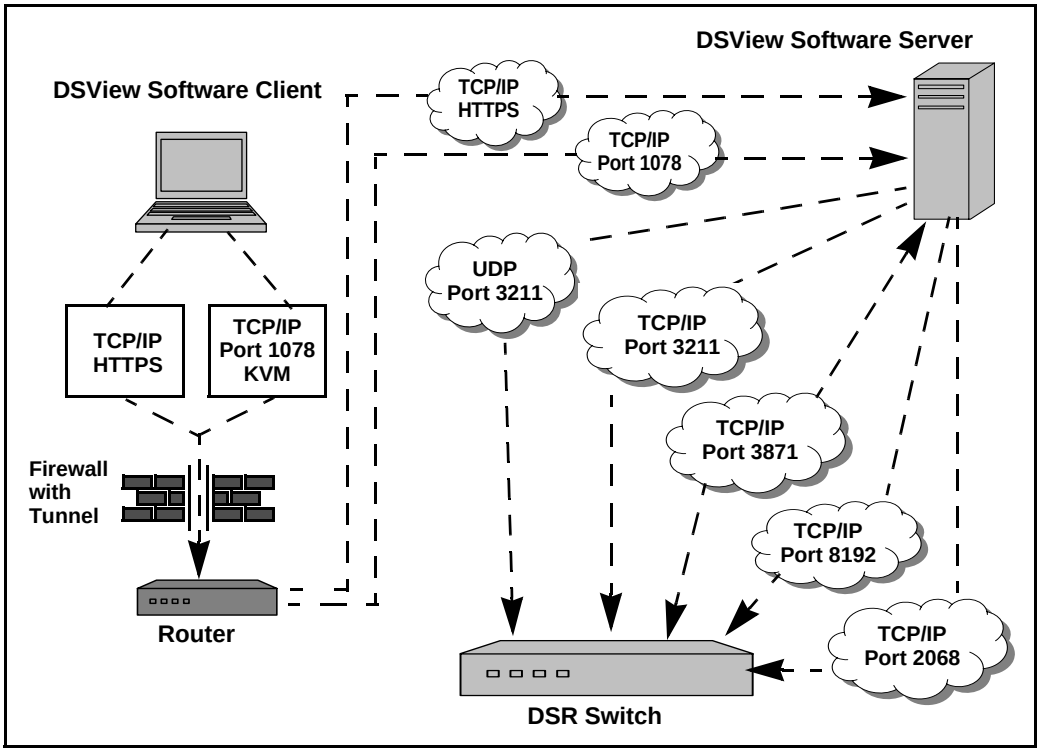


Figure B.2: Ports Used with a DS1800 Digital Switch or DSR Switch Proxy Server Connection (KVM)

If the user wishes to establish a session with another port on the DS1800 digital switch or DSR switch, the same process is used.

For debugging purposes, connection details may be seen by using the console port to place the DS1800 digital switch or DSR switch into Debug mode.

CPS and CCM appliance ports

Like a DS1800 digital switch or DSR switch, a CPS or CCM appliance may use a non-proxied or a proxied connection. CPS and CCM appliances use a Secure Shell Protocol (SSH).

The client contacts the server, which checks the permissions of the target device. If the logged in user has permissions to establish sessions to the selected target device, the server will establish a connection to the appliance using TCP/IP port 3871 to authorize the session.

In a non-proxied SSH connection, the client communicates directly with the appliance using port 22. Figure B.3 illustrates the ports used with a non-proxied CPS/CCM appliance connection.

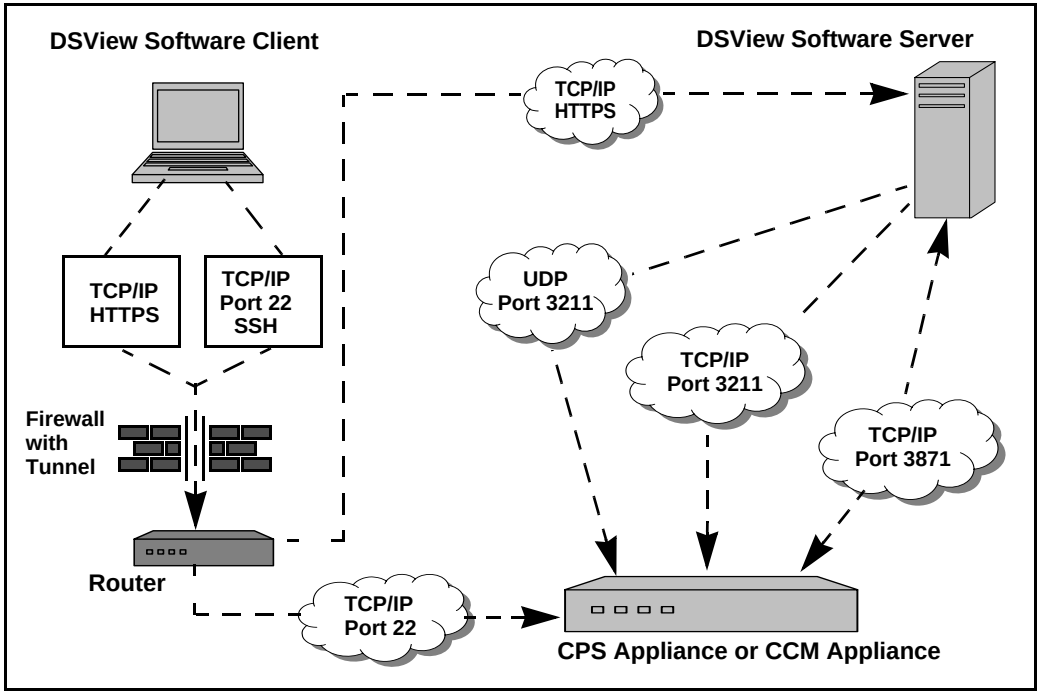


Figure B.3: Ports Used with a CPS or CCM Appliance Connection (Serial) Without Proxy

In a proxied connection, communication between the DSView software server and CPS or CCM appliance occurs over port 22. The SSH connection between the client and the DSView software server is tunneled over port 1078. Figure B.4 illustrates the ports used with a proxied CPS or CCM appliance connection.

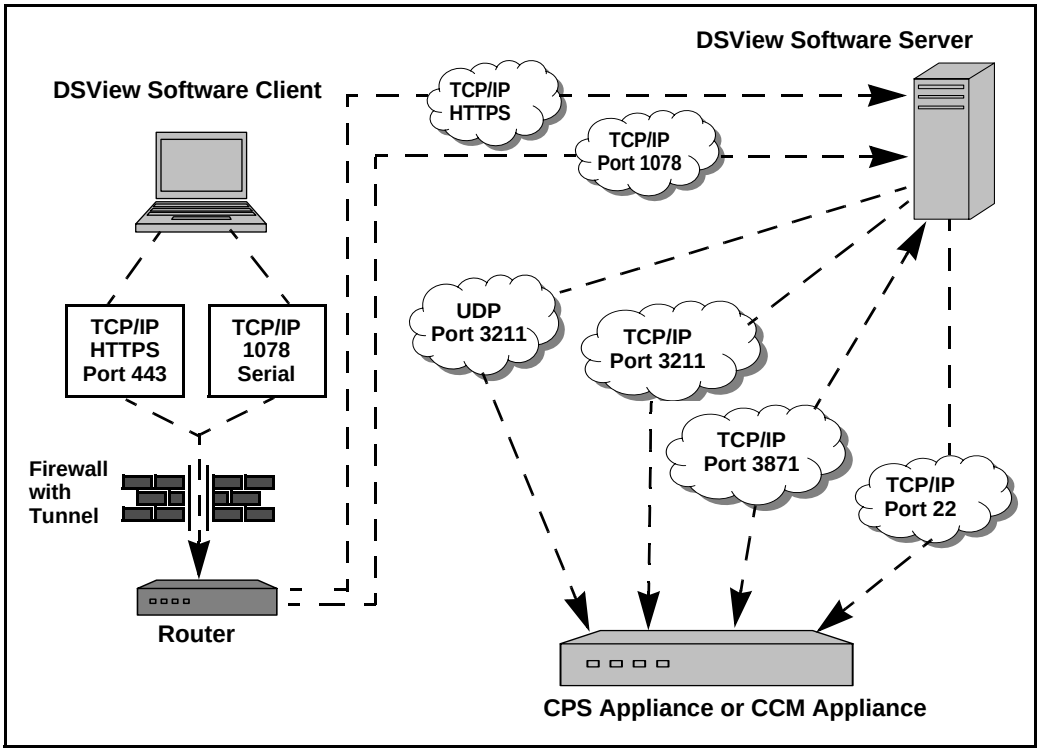


Figure B.4: Ports Used with a CPS or CCM Appliance Proxy Server Connection (Serial)

DSView software server ports

The DSView software server uses the HTTPS port for communication with clients and spoke servers. Changes made to the browse list through the DSView management software are transmitted back to the DSView software server host, which refreshes its browse list view over the TCP/IP port 443 connection. Changes to the DSView management software are also copied to and from the DSView software hub server over the specified HTTPS port.

Generic appliance ports

If you are using a generic appliance in your DSView software system, you may use a Telnet connection through TCP/IP port 23, or an HTTP connection through TCP/IP port 80. The connection is made directly between the client and the generic appliance.

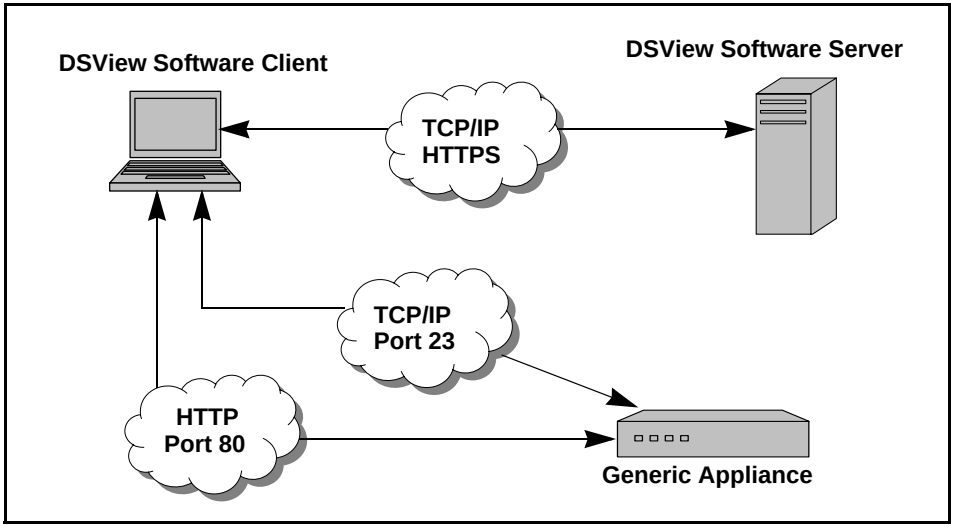


Figure B.5: Generic Appliance Session Ports

If Active Directory or LDAP external authentication is being used within your DSView software system, TCP/IP ports 389 and 636 are used for connections between the DSView software server and the external authentication server. Port 389 is typically used for non-SSL connections and port 636 is used for SSL connections. You may configure the ports used by an Active Directory or LDAP external authentication server using the Authentication Service Connection Settings window. See *Managing Authentication Services* on page 58 for more information.

External authentication ports

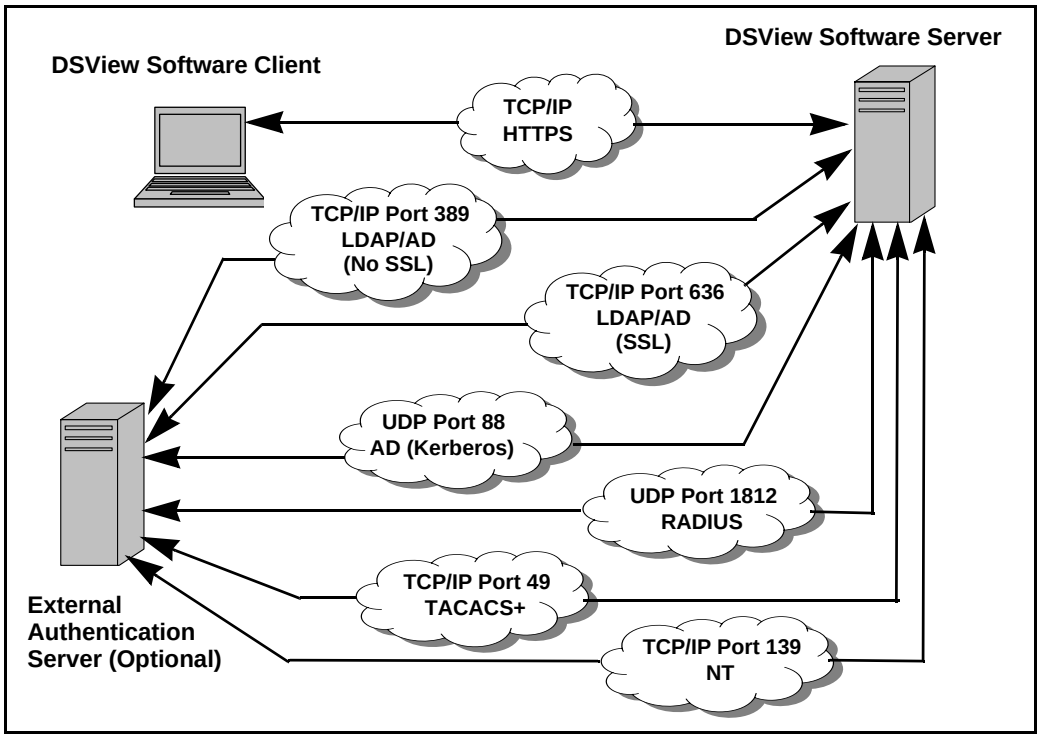


Figure B.6: External Authentication Server Ports

SNMP ports

A DS1800 digital switch, DSR switch, CPS appliance or CCM appliance may be configured to send SNMP traps to the DSView software server in addition to an external SNMP manager.

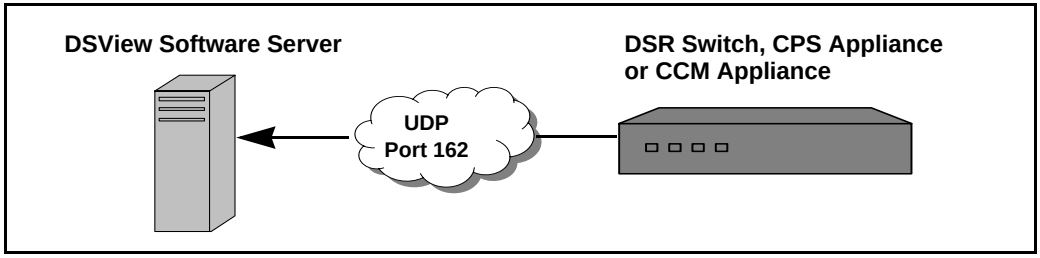


Figure B.7: Ports Used by SNMP (No External SNMP Manager)

If an external SNMP manager has been added to your DSView software system, communication occurs between the SNMP manager and the DS1800 digital switch, DSR switch, CPS appliance or CCM appliance as shown in Figure B.8.

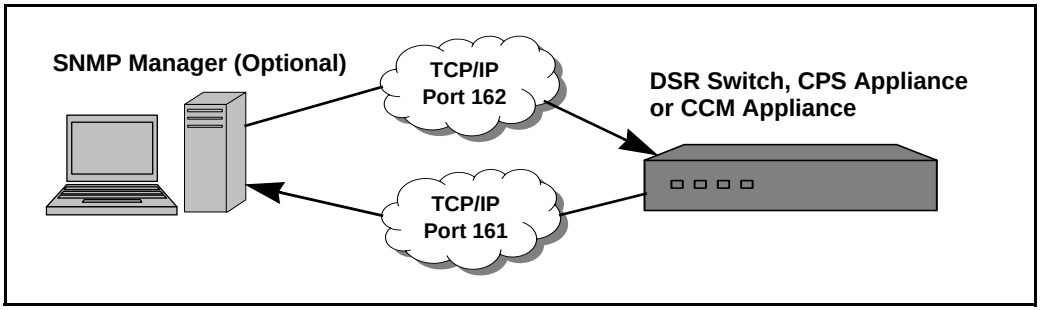


Figure B.8: Ports Used by SNMP (with External SNMP Manager)

DSI5100 IPMI proxy appliance ports

If a DSI5100 appliance is being used within your DSView software system, TCP/IP ports 3871 and 3502 are used for connections between the DSView software server and the DSI5100 proxy appliance. Port 3871 is used for certificate exchanges and port 3502 is used for data exchanges. UDP port 623 is used for communications between the DSI5100 proxy appliance and any configured BMCs. When a BMC is selected for viewing in the DSView management software using the IPMI Viewer window, TCP/IP port 443 is used for communication between the DSView management software and the server.

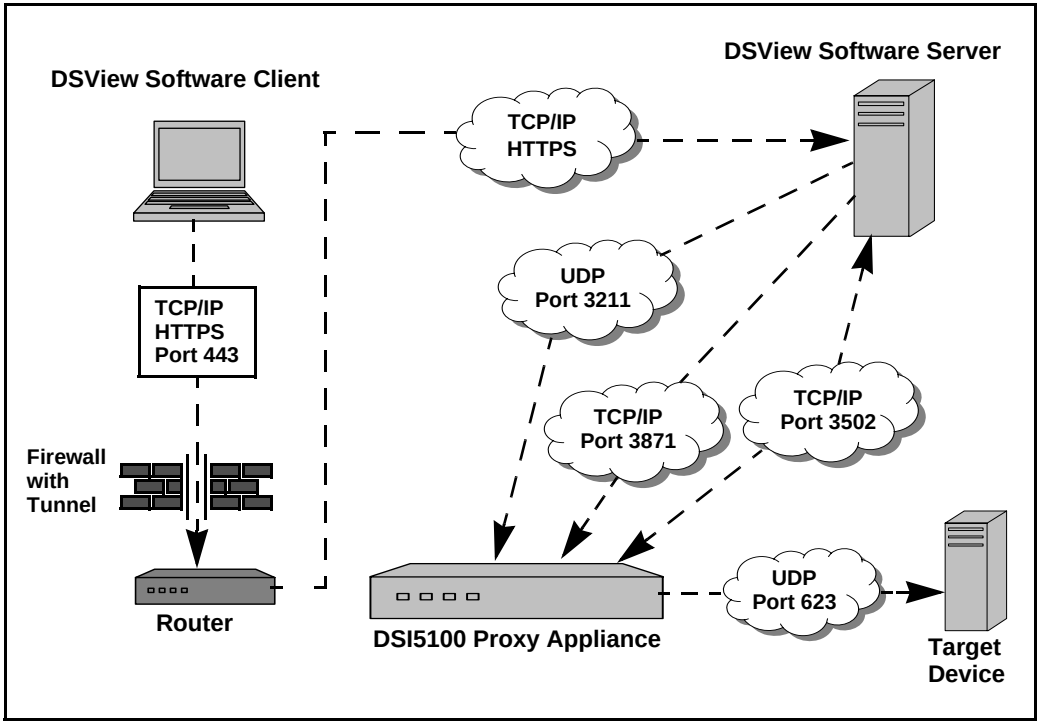


Figure B.9: Ports Used by DSI5100 Appliances

Appendix C: DSR Remote Operations Software

NOTE: The DSR Remote Operations software is supported only on the following DSR switches: DSR1020, 1021, 1022, 1024, 1030, 1031, 2020, 2030, 2035, 4020, 4030, 8020, 8030 and 8035 switches.

The DSR Remote Operations software provides a subset of DSView management software functionality that allows access to a supported DSR switch when an Ethernet connection is not available. For example, if you are in a branch office and your Ethernet network is down, you may still access your remote server network by attaching a v.34, v.90 or v.92-compatible modem to the modem port on a supported DSR switch for KVM access, administration and flexible server management control from anywhere in the world.

The following DSView management software operations are supported:

- Establishing a KVM session to a target device connected to the switch
- Controlling the power sockets of an SPC device attached to the DSR switch power port
- Rebooting the switch
- Retrieving and displaying the switch version

All other DSView management software options (including using virtual media) are not available when using the DSR Remote Operations software.

The following Video Viewer window commands are not available when using the DSR Remote Operations software:

- Displaying connected user information
- Creating, editing, copying and deleting macros

NOTE: Only the default Windows and Sun macro groups are available when using the Remote Operations software.

- Background refresh

An external modem must be attached to the PPP modem interface of the DSR switch to use the DSR Remote Operations software. A modem/PPP dial-up connection must be established before the DSR Remote Operations software may be started, run or executed. The dial-up connection options should be set to 115200 baud, 8 bits, 1 stop bit, no parity and enabled hardware flow control. The remote operations application must be started within the authentication time-out specified in the Terminal Applications menu of the DSR switch or the PPP (modem) link will be disconnected. See the DSR Switch Installer/User Guide for more information.

Once a modem dial-up connection is established with the switch, select *Start - Programs - Avocent DSView 3.0 - DSR Remote Operations* on a client computer containing the software.

Log in using a valid username and password to establish a DSR Remote Operations software session with the DSR switch over the modem link.

The DSR Remote Operations software uses an SSL-based connection to the DSR switch to authenticate the user.

If the DSView software server is unreachable, the switch will use its internal database to perform remote authentication. If the internal database of the DSR switch fails to authenticate the user when a login is attempted, or the user does not log in before the specified time-out of the DSR switch, the modem connection will be disconnected.

NOTE: Users may be managed within the internal database of the DSR switch using the PPP Configuration menu. See the installer/user guide for your DSR switch for more information.

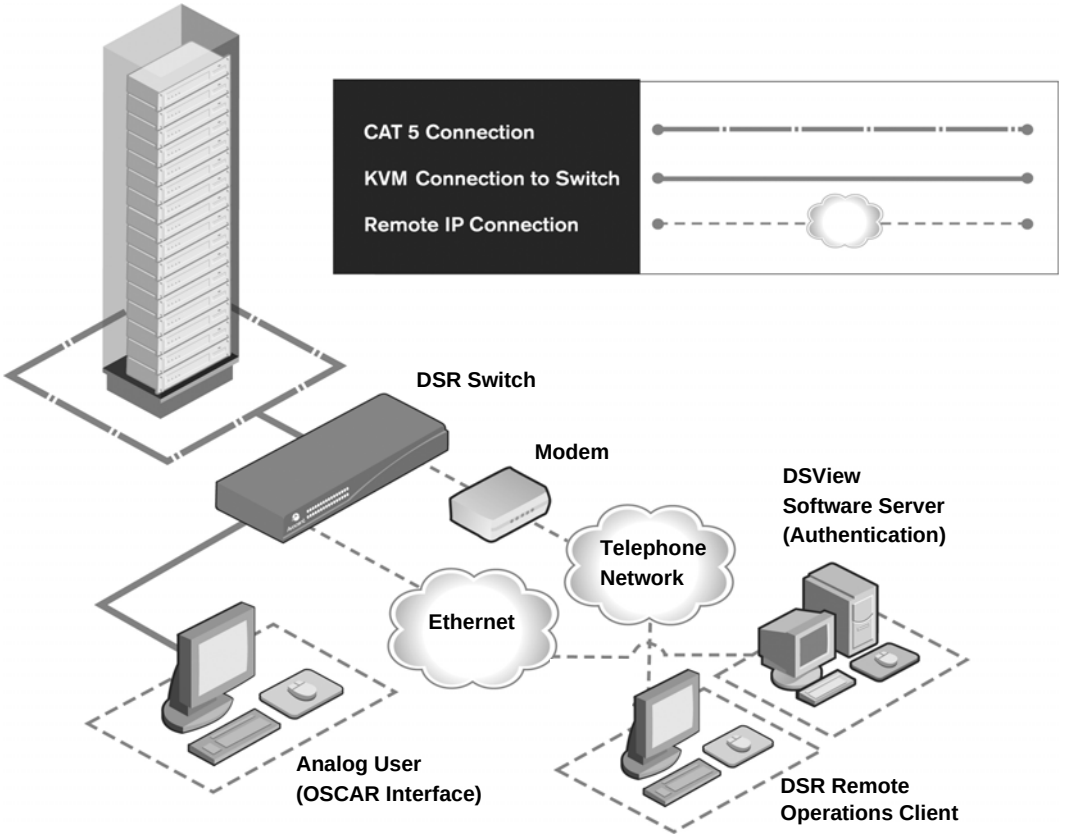


Figure C.1: Using the DSR Remote Operations Software with a DSR Switch

See *Installing the DSR Remote Operations Software (Optional)* on page 43 for more information.

DSR Remote Operations window features

When you have launched the software and successfully logged in, the DSR Remote Operations window will display the list of DSView software servers connected to the DSR switch. Figure C.2 shows the DSR Remote Operations window areas, and descriptions follow in Table C.1.

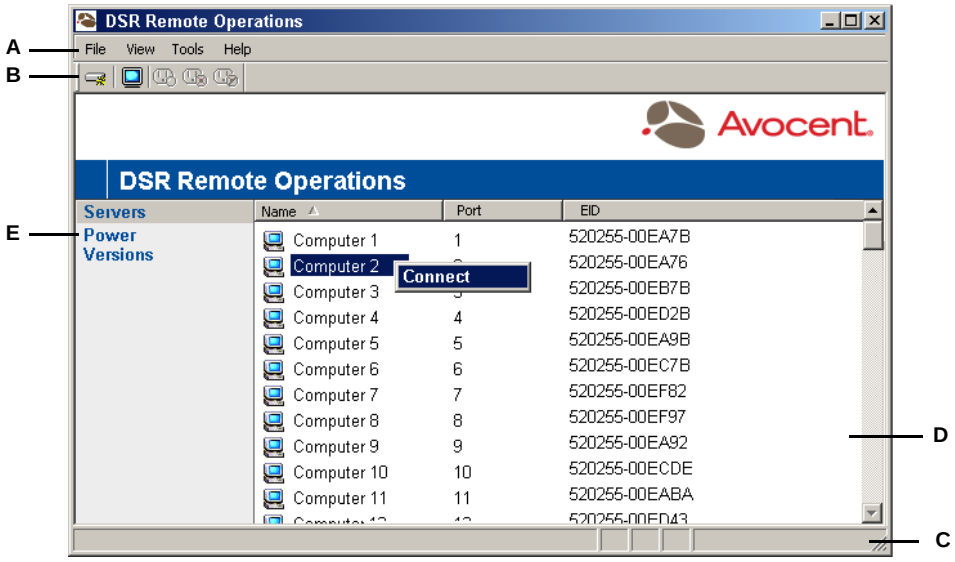


Figure C.2: DSR Remote Operations Window

Table C.1: DSR Remote Operations Descriptions

Letter	Description
A	Menu bar: Allows you to access many of the features in the DSR Remote Operations window.
B	Toolbar: Provides shortcut buttons for quickly accessing commands in the Tools menu.
C	Status Bar: Displays the tips for selected menu items and the progress of operations.
D	Content Area: Use this area to display information from the DSR switch and control and start DSView software sessions to the DSR switch.
E	Side Navigation Bar: Displays the DSR switching system information you wish to access, which displays in the Content Area.

Content area views

The items displayed in the content area of the DSR Remote Operations window will vary, depending on which link has been selected in the side navigation bar.

Servers view

When *Servers* is selected, a list of servers attached to the switch will appear. The following items for each server will appear in the content area:

- Name - The name of the server
- Port - The switch port to which the server is attached

- EID - The Electronic ID (EID) number of the DSRIQ module attached to the server

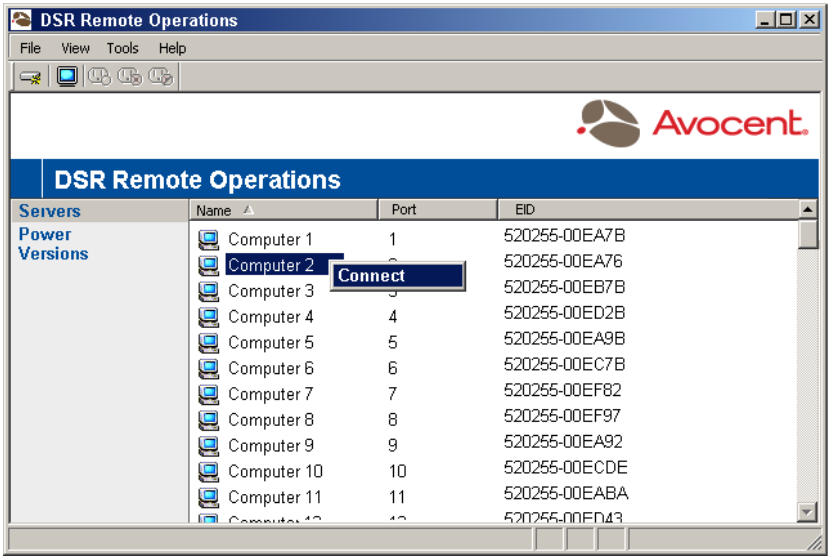


Figure C.3: DSR Remote Operations Window (Servers View)

Specific icons also appear in the Server view. These icons are outlined in Table C.2.

Table C.2: DSR Remote Operations Content Area Icons (Servers View)

Icon	Description
	A target device that is powered up and has no established KVM Video Viewer sessions
	A target device that has an active KVM Video Viewer session
	A target device that is not powered up
	A target device that is powered up but cannot establish a KVM connection because the path to the target device is blocked (for example, a cascade switch has only one user port and that port is already connected to another target device)

Power view

Selecting *Power* in the side navigation bar of the DSR Remote Operations window will display a list of SPC device sockets attached to the switch and their powered up or powered down status.

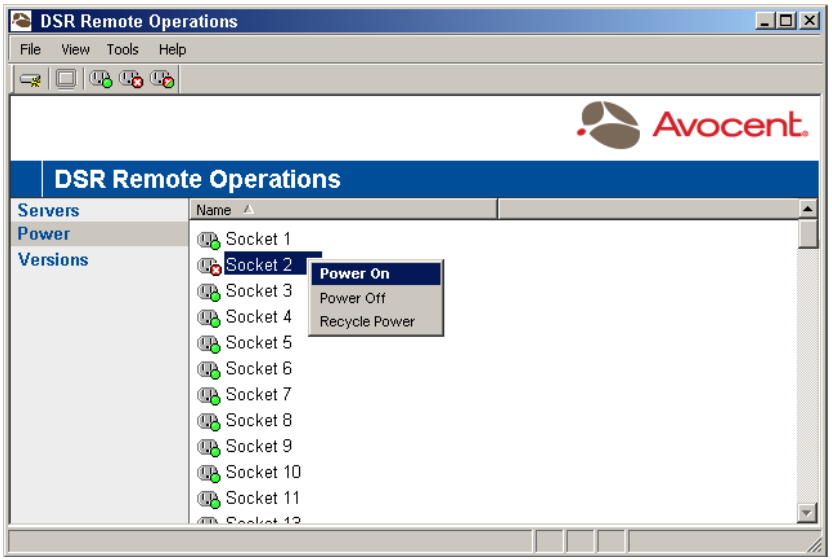


Figure C.4: DSR Remote Operations Window (Power View)

Specific icons also appear in the Power view. These icons are outlined in Table C.3.

Table C.3: DSR Remote Operations Content Area Icons (Power View)

Icon	Description
	The SPC device socket is powered up
	The SPC device socket is powered down

Version view

Selecting *Version* in the side navigation bar of the DSR Remote Operations window will display version information for the switch.

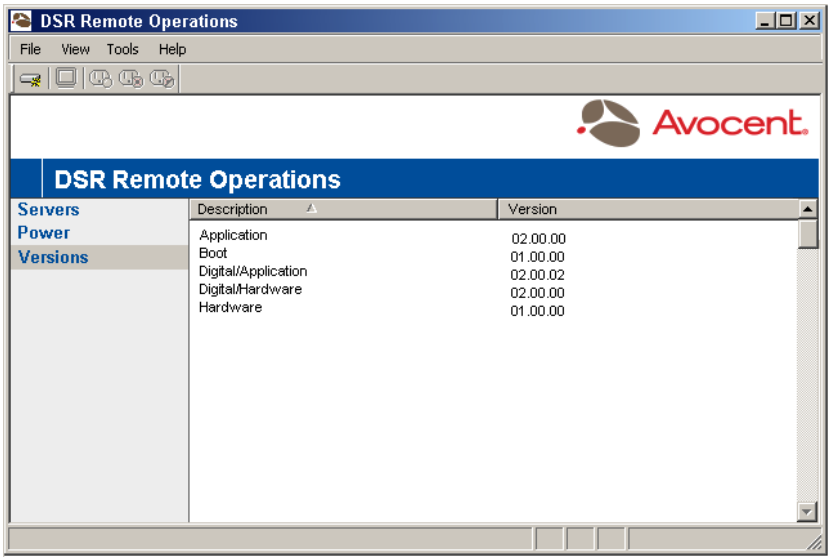


Figure C.5: DSR Remote Operations Window (Versions View)

Before you begin

The following actions should be performed before using the DSR Remote Operations command:

- Ensure that the switch is configured. See the installer/user guide for the DSR switch for more information.
- Ensure that users have been added to the internal database of the DSR switch. If the DSView software server is not available, the appliance database is used for appliance authentication. If neither are available, authentication cannot be performed for the switch and an error will be displayed by the DSR Remote Operations software. See the installer/user guide for the DSR switch for more information.
- Ensure that an external modem is attached to the modem port of the DSR switch. The modem port should have auto-answer turned off (typically a modem's default setting).
- Ensure that the PC containing the client interface has dial-up software and that the software is configured properly. See the operating system documentation for more information.
- Ensure that you are using one of the following supported operating systems: Windows NT 4.0 Workstation or Server with Service Pack 6a or later; Windows 2000 Workstation or Server with Service Pack 2 or later; or Windows XP Home Edition or Professional.

To use the DSR Remote Operations command:

1. Establish a dial-up connection to the switch from the PC containing the DSR remote operations software.

NOTE: Windows displays a dialog box that prompts the user for a username and password when a dial-up connection is established. It is not necessary to enter a username or password in the dialog box. When this dialog box appears, click *OK* to close the dialog box.

2. Once the connection has been established, select *Start - Programs - Avocent DSView 3.0 - DSR Remote Operations* to start the DSR Remote Operations software on the PC. The Login dialog box will appear.

   The switch will disconnect the modem connection if a user does not log in within the time period specified by the authentication time-out value. The default authentication time-out value (120 seconds) may be changed using the Terminal Applications menu. See the installer/user guide for the DSR switch for more information.

   The DSR switch will attempt to contact the DSView software server to authenticate the user. If the DSView software server is unavailable, the switch will use its internal database to authenticate the user.

3. Type the username and password to which you wish to connect and then click *OK*. If authentication is successful, the DSR Remote Operations window will open.

NOTE: The switch will disconnect the modem connection if there is no activity on the modem connection for the time period specified by the inactivity time-out value. The default inactivity time-out value (15 minutes) may be changed using the Terminal Applications menu. See the installer/user guide for the DSR switch for more information.

Rebooting a switch

NOTE: Users with a User level account may not reboot a switch.

To reboot the switch:

1. In the menu bar, select *Tools - Reboot Appliance*. A confirmation dialog box will appear.
2. Click *Yes* to reboot the switch.

   -or-

   Click *No* to cancel the operation.

Managing servers

Use the Servers view to manage servers attached to the switch. See *Servers view* on page 303 for more information.

To display the Servers view:

In the menu bar, select *View - Servers*.

-or-

In the side navigation bar, click *Servers*.

To refresh the Server view:

In the menu bar when the Servers view is displayed, select *View* - *Refresh.*

To connect to a server:

NOTE: Users with a User level account may connect to a server only when given access to a switch. See *Built-in User Groups* on page 22 for more information.

From the Servers view, select a server and select *Tools* - *Connect* from the menu bar.

-or-

Select a server and click the *Connect* toolbar button.

-or-

Right-click on a server and select *Connect* from the shortcut menu.

A Video Viewer window will open. See *Using the Video Viewer* on page 171 for more information.

The following operations are unavailable when using the DSR Remote Operations command:

- Sharing (see *Connecting to an existing KVM session* on page 267 for more information)
- Stealth connections (see *Connecting to an existing session* on page 173 for more information)
- Scan Mode (enabled when two or more Video Viewer windows are open)
- Macro Creation (Macros - Configure from the Video Viewer window menu bar)
- View Connected Users (View - Connected Users from the Video Viewer window menu bar)

Managing SPC device sockets

Users with User level account privileges cannot change the power state of SPC device sockets. See *Built-in User Groups* on page 22 for more information.

Use the Power view to manage SPC device sockets attached to the switch. See *Power view* on page 304 for more information.

To display the Power view:

In the menu bar, click *View* - *Power*.

-or-

In the side navigation bar, click *Power*.

To refresh the Power view:

Select *View* - *Refresh* from the menu bar when the Power view is displayed.

To power up an SPC device socket:

1. Click *Power* in the side navigation bar. A list of SPC device sockets attached to the switch will appear in the content area.
2. Select an SPC device socket that has not been powered up and select *Tools* - *Power On* from the menu bar.

-or-

Select an SPC device socket that has not been powered up and click the *Power On* toolbar button.

-or-

Right-click on an SPC device socket that has not been powered up and select *Power On* from the shortcut menu.

The SPC device socket will power up and the icon for the SPC device socket in the content area will change.

To power down an SPC device socket:

1. Click *Power* in the side navigation bar. A list of SPC device sockets attached to the switch will appear in the content area.
2. Select an SPC device socket that has not been powered down and select *Tools - Power Off* from the menu bar.

   -or-

   Select an SPC device socket that has not been powered down and click the *Power Off* toolbar button.

   -or-

   Right-click on an SPC device socket that has not been powered down and select *Power Off* from the shortcut menu.

   The SPC device socket will power down and the icon for the SPC device socket in the content area will change.

To cycle the power of an SPC device socket:

1. Click *Power* in the side navigation bar. A list of SPC device sockets attached to the switch will appear in the content area.
2. Select an SPC device socket that is powered up and select *Tools - Cycle Power* from the menu bar.

   -or-

   Select an SPC device socket that is powered up and click the *Cycle Power* toolbar button.

   -or-

   Right-click on an SPC device socket that is powered up and select *Cycle Power* from the shortcut menu.

   The SPC device socket is powered down, then powered up and the icon for the SPC device socket in the content area will change accordingly.

Displaying switch version information

To display switch version information:

In the menu bar, select *View - Versions.*

-or-

In the side navigation bar, click *Version*. The versions of the following items will appear in the content area:

- Application
- Boot
- Digital/Application
- Digital/Hardware
- Hardware

To refresh the Versions view:

In the menu bar when the Versions view is displayed, select *View* - *Refresh*.

Exiting DSR Remote Operations

To exit DSR remote operations:

In the menu bar, select *File* - *Exit*.

Appendix D: Terminal Emulation

This appendix contains information about the keys, sequences, encoding and decoding for the DSView management software terminal emulation modes when using the Telnet Viewer. Encode refers to how the client interface processes typed keys. Decode refers to how the client interface processes data coming from the target device.

The terminal emulation mode is set by selecting *Options - Session Properties* in the Telnet Viewer window and then using the Terminal Emulation drop-down menu in the Session Properties dialog box. See *Customizing Session Properties* on page 212 for more information.

VT terminal emulation

Table D.1 lists the VT key and keypad numeric codes. Avocent encodes all applicable keys as numeric; decoding is not supported.

Table D.1: VT Key and Keypad Numeric Codes

Key	Keypad Numeric Code
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
- (dash)	- (dash)
, (comma)	, (comma)
. (period)	. (period)
Enter	Same as Return key

VT100+ terminal emulation

The VT100+ emulation provides compatibility with the Microsoft headless server EMS serial port interface. The DSView software Telnet Viewer VT100+ terminal emulation works identically to VT100, with the exception of support for the function keys listed in Table D.2.

Table D.2: VT100+ Function Key Support

Function	Sequence	Function	Sequence
Home	<Esc> h	F4 **	<Esc> 4
End	<Esc> k	F5	<Esc> 5
Insert	<Esc> +	F6	<Esc> 6
Delete *	<Esc> -	F7	<Esc> 7
Page Up	<Esc> ?	F8	<Esc> 8
Page Down	<Esc> /	F9	<Esc> 9
F1 **	<Esc> 1	F10	<Esc> 0
F2 **	<Esc> 2	F11	<Esc> !
F3 **	<Esc> 3	F12	<Esc> @

* ASCII, VT52, VT100, VT102, VT220 and VT320 modes send hex 7F when the **Delete** key is pressed.
** VT100, VT102, VT220 and VT320 modes map the **F1**-**F4** keys to the **PF1**-**PF4** keys.

VT102 terminal emulation

VT102 terminal emulation works identically to VT100 with additional support for decoding receive codes as described in Table D.3.

Table D.3: VT102 Receive Codes

VT102 Receive Code	Action
Delete Character (DHC)	Deletes n characters starting with the character at the current cursor position, and moves all remaining characters left n positions. n spaces are inserted at the right margin.
Insert Line (IL)	Inserts n lines at the line where the cursor is currently positioned. Lines displayed below the cursor position move down. Lines moved past the bottom margin are lost.
Delete Line (DL)	Deletes n lines starting with the line where the cursor is currently positioned. As lines are deleted, lines below the cursor position move up.

VT100 terminal emulation

Table D.4 lists the VT100 special key and control (**Ctrl**) key combinations and indicates Avocent encoding/decoding support, where Yes = supported and No = not supported.

Table D.4: VT100 Special Keys and Control Keys

Keys	Hex Code	Function Mnemonic	Encode/Decode
Return	0D	CR	Yes/Yes
Linefeed	0A	LF	Yes/Yes
Backspace	08	BS	Yes/Yes
Tab	09	HT	Yes/Yes
Spacebar	20	(SP)	Yes/Yes
Esc	1B	Esc	Yes/No
Ctrl+Spacebar	00	NUL	Yes/No
Ctrl+A	01	SOH	Yes/No
Ctrl+B	02	STX	Yes/No
Ctrl+C	03	ETX	Yes/No
Ctrl+D	04	EOT	Yes/No
Ctrl+E	05	ENO	Yes/No
Ctrl+F	06	ACK	Yes/No
Ctrl+G	07	BELL	Yes/Yes
Ctrl+H	08	BS	Yes/Yes
Ctrl+I	09	HT	Yes/Yes
Ctrl+J	0A	LF	Yes/Yes
Ctrl+K	0B	VT	Yes/No
Ctrl+L	0C	FF	Yes/No
Ctrl+M	0D	CR	Yes/No
Ctrl+N	0E	SO	Yes/No
Ctrl+O	0F	SI	Yes/No
Ctrl+P	10	DLE	Yes/No
Ctrl+Q	11	DC1 or XON	Yes/No

Table D.4: VT100 Special Keys and Control Keys (Continued)

Keys	Hex Code	Function Mnemonic	Encode/Decode
Ctrl+R	12	DC2	Yes/No
Ctrl+S	13	DC3 or XOFF	Yes/No
Ctrl+T	14	DO4	Yes/No
Ctrl+U	15	NAK	Yes/No
Ctrl+V	16	SYN	Yes/No
Ctrl+W	17	ETB	Yes/No
Ctrl+X	18	CAN	Yes/No
Ctrl+Y	19	EM	Yes/No
Ctrl+Z	1A	SUB	Yes/No
Ctrl+[	1B	Esc	Yes/No
Ctrl+\	1C	FS	Yes/No
Ctrl+]	1D	GS	Yes/No
Ctrl+^	1E	RS	Yes/No
Ctrl+_	1F	US	Yes/No

Table D.5 lists the VT100 ANSI mode and cursor keys for set and reset modes. Encoding and decoding is supported for all the cursor keys listed.

Table D.5: VT100 ANSI Set and Reset Mode Cursor Keys

Cursor Key	Mode Reset	Mode Set
Up	Esc [A	Esc O A
Down	Esc [B	Esc O B
Right	Esc [C	Esc O C
Left	Esc [D	Esc O D

Table D.6 lists the VT100 PF1-PF4 key definitions. Encoding of each listed key is supported; decoding is not applicable.

Table D.6: VT100 PF1-PF4 Key Definitions

Key	Code Sequence
F1	Esc [O P
F2	Esc [O Q
F3	Esc [O R
F4	Esc [O S

Table D.7 lists the ANSI mode control sequences for VT100 terminal emulation and indicates Avocent encoding/decoding support, where Yes = supported and No = not supported.

Table D.7: VT100 ANSI Mode Control Sequences

Control Sequence	Definition	Encode/Decode
Esc [Pn; Pn R	Cursor Position Report	No/No
Esc [Pn D	Cursor Backward	No/Yes
Esc [Pn B	Cursor Down	No/Yes
Esc [Pn C	Cursor Forward	No/Yes
Esc [Pn; Pn H	Cursor Position	No/Yes
Esc [Pn A	Cursor Up	No/Yes
Esc [Pn c	Device Attributes	No/No
Esc # 8	Screen Alignment Display	No/Yes
Esc # 3	Double Height Line - Top Half	No/No
Esc # 4	Double Height Line - Bottom Half	No/No
Esc # 6	Double Width Line	No/No
Esc Z	Identify Terminal	No/No
Esc =	Keypad Application Mode	No/No
Esc >	Keypad Numeric Mode	No/No
Esc [Ps q	Load LEDs	No/No
Esc 8	Restore Cursor	No/Yes

Table D.7: VT100 ANSI Mode Control Sequences (Continued)

Control Sequence	Definition	Encode/Decode
Esc [<sol>; <par>;	Report Terminal Parameters <nbits>; <xspeed>; <rspeed>; <clkmul>; <flags>x	No/No
Esc [<sol> x	Request Terminal Parameters	No/No
Esc 7	Save Cursor	No/Yes
Esc [Pn; Pn r	Set Top and Bottom Margins	Yes/Yes
Esc # 5	Single Width Line	No/No
Esc [2; Ps y	Invoke Confidence Test	No/No
Esc [Ps n	Device Status Report	No/Yes
Esc [Ps J	Erase in Display	No/Yes
Esc [Ps K	Erase in Line	No/Yes
Esc H	Horizontal Tabulation Set	Yes/Yes
Esc [Pn; Pn f	Horizontal and Vertical Position	No/Yes
Esc D	Index	No/Yes
Esc E	Next Line	No/Yes
Esc M	Reverse Index	No/Yes
Esc c	Reset to Initial State	No/No
Esc [Ps; Ps;..;Ps 1	Reset Mode	No/No
Esc (A	Select Character Set GØ U.K.	No/No
Esc) A	Select Character Set G1 U.K	No/No
Esc (B	Select Character Set GØ ASCII	Yes/Yes
Esc) B	Select Character Set G1 ASCII	Yes/Yes (limited support)
Esc (0	Select Character Set G0 Spec. Graphics	Yes/Yes (limited support)
Esc) 0	Select Character Set G1 Spec. Graphics	Yes/Yes (limited support)
Esc (1	Select Character Set G0 Alt. Character ROM Standard Character Set	No/No
Esc) 1	Select Character Set G1 Alt. Character ROM Standard Character Set	No/No
Esc (2	Select Character Set G0 Alt. Character ROM Special Graphics	No/No

Table D.7: VT100 ANSI Mode Control Sequences (Continued)

Control Sequence	Definition	Encode/Decode
Esc) 2	Select Character Set G1 Alt. Character ROM Special Graphics	No/No
Esc [Ps;..; Ps m	Select Graphic Rendition	No/No
Esc Ps;..;Ps h	Set Mode	No/No
Esc [Ps g	Tabulation Clear	No/No
Esc [Ps;Ps;..; Ps m	Character Attributes 7 - Reverse Video On	No/Reverse Video only
Esc [K or Esc [0 K	Erase from cursor to end of line	No/Yes
Esc [1 K	Erase from beginning of line to cursor	No/No
Esc [2 K	Erase entire line containing cursor	No/No
Esc [J or Esc [0 J	Erase from cursor to end of screen	No/Yes
Esc [1 J	Erase from beginning of screen to cursor	No/No
Esc [2 J	Erase entire screen	No/No
Esc [Ps;Ps;..Ps q	Programmable LEDs	No/No
Esc [Pt; Pb r	Scrolling Region	No/No
Esc [g or Esc [0 g	Clear tab at current column	Yes/Yes
Esc [3 g	Clear all tabs	Yes/Yes
Esc [2 0 h	Modes to Set - New Line - Only supports Linefeed/ New Line Column mode wraparound	No/Yes
Esc [2 0 l	Modes to Reset - Linefeed - Only supports Linefeed/ New Line Column mode wraparound	No/Yes
Esc [? 1 h	Modes to Set - Cursor Key Mode Appl.	No/No
Esc [? 1 l	Modes to Reset - Cursor Key Mode Cursor	No/No
Esc [? 2 l	Modes to Reset VT52	No/No
Esc [? 3 h	Modes to Set - 132 columns	No/No
Esc [? 3 l	Modes to Reset - 80 columns	No/No
Esc [? 4 h	Modes to Set - Smooth Scroll	No/No
Esc [? 4 l	Modes to Reset - Jump Scroll	No/No
Esc [? 5 h	Modes to Set - Reverse Screen Mode	No/No

Table D.7: VT100 ANSI Mode Control Sequences (Continued)

Control Sequence	Definition	Encode/Decode
Esc [? 5 l	Modes to Reset - Normal Screen Mode	No/No
Esc [? 6 h	Modes to Set - Relative Origin Mode	No/No
Esc [? 6 l	Modes to Reset - Absolute Origin Mode	No/No
Esc [? 7 h	Modes to Set - Wraparound On	No/No
Esc [? 7 l	Modes to Reset - Wraparound Off	No/No
Esc [? 8 h	Modes to Set - Auto Repeat On	No/No
Esc [? 8 l	Modes to Reset - Auto Repeat Off	No/No
Esc [? 9 h	Modes to Set - Interlace On	No/No
Esc [? 9 l	Modes to Reset - Interlace Off	No/No
Esc [6 n	Report Cursor Position - Invoked by	No/No
Esc [P1; Pc R	Report Cursor Position - Response is	No/No
Esc [5 n	Status Report - Invoked by	No/No
Esc [0 n	Status Report - Response is terminal OK	No/No
Esc [3 n	Status Report - Response is terminal not OK	No/No
Esc [x or Esc [0 c	What are you? Invoked by	No/Yes
Esc [? 1; Ps c	What are you? Response is	No/Yes
Esc c	Reset	No/No
Esc # 8	Fill screen with Es	No/Yes
Esc [2; Ps y	Invoke Test(s)	No/No

VT220 terminal emulation

Table D.8 lists the keystroke mapping (encoding) for VT220 emulation.

Table D.8: VT220 Encoding

VT220 Keyboard	PC Keyboard	VT220 Keyboard Byte Sequence
Delete	Delete	0x7F
Left Arrow	Left Arrow	Esc [D
Right Arrow	Right Arrow	Esc [C
Up Arrow	Up Arrow	Esc [A
Down Arrow	Down Arrow	Esc [B
Keypad /	Keypad /	/
Keypad *	Keypad *	*
Keypad -	Keypad -	-
Keypad +	Keypad +	+
Keypad .	Keypad .	.
Keypad 0..9	Keypad 0..9	0..9
F1	F1	Esc O P
F2	F2	Esc O Q
F3	F3	Esc O R
F4	F4	Esc O S
F6	F6	Esc [1 7 ~
F7	F7	Esc [1 8 ~
F8	F8	Esc [1 9 ~
F9	F9	Esc [2 0 ~
F10	F10	Esc [2 1 ~
F11	F11	Esc [2 3 ~
F12	F12	Esc [2 4 ~
F13	Ctrl - F5	Esc [2 5 ~
F14	Ctrl - F6	Esc [2 6 ~

Table D.8: VT220 Encoding (Continued)

VT220 Keyboard	PC Keyboard	VT220 Keyboard Byte Sequence
F15	Ctrl - F7	Esc [2 8 ~
F16	Ctrl - F8	Esc [2 9 ~
F17	Ctrl - F9	Esc [3 1 ~
F18	Ctrl - F10	Esc [3 2 ~
F19	Ctrl - F11	Esc [3 3 ~
F20	Ctrl - F12	Esc [3 4 ~

Table D.9 lists the decoding for VT220 terminal emulation.

Table D.9: VT220 Decoding

VT220 Keyboard Function	VT220 Keyboard Byte Sequence
Index	Esc D
New Line	Esc E
Reverse Index	Esc M
Escape	Esc O
Save cursor and attributes	Esc 7
Restore cursor and attributes	Esc 8
Up Arrow	Esc [A
Down Arrow	Esc [B
Right Arrow	Esc [C
Left Arrow	Esc [D
Set cursor to home position	Esc [H
Set cursor to home position	Esc [f
Character attributes	Esc [m
Erase from cursor to end of line	Esc [K
Erase from cursor to end of screen	Esc [j
Programmable LEDs	Esc [q
What are You?	Esc [c

Table D.9: VT220 Decoding (Continued)

VT220 Keyboard Function	VT220 Keyboard Byte Sequence
Set Mode	Esc [?
Delete 1 Character	Esc [P
Insert 1 Line	Esc [L
Delete 1 Line	Esc [M
Up Arrow	Esc [O A
Down Arrow	Esc [O B
Right Arrow	Esc [O C
Left Arrow	Esc [O D
Fill Screen with Es	Esc # 8
Up Arrow amount specified by Pn	Esc [Pn A
Down Arrow amount specified by Pn	Esc [Pn B
Right Arrow amount specified by Pn	Esc [Pn C
Left Arrow amount specified by Pn	Esc [Pn D
Erase parts of current line	Esc [Pn K
Erase parts of current screen	Esc [Pn J
Direct Cursor Addressing	Esc [Pn H
Direct Cursor Addressing	Esc [Pn f
Programmable LEDs	Esc [Pn q
Scrolling Region	Esc [Pn r
Clear tabs	Esc [Pn g
Device status report	Esc [Pn n
What are you?	Esc [Pn c
Sat Mode	Esc [Pn h
Delete Pn Characters	Esc [Pn P
Insert Pn Characters	Esc [Pn L
Delete Pn Lines	Esc [Pn M
Insert Character	Esc [Pn @

Table D.9: VT220 Decoding (Continued)

VT220 Keyboard Function	VT220 Keyboard Byte Sequence
Erase Pn Characters	Esc [Pn X

VT52 terminal emulation

Table D.10 lists the keystroke mapping (encoding) for VT52 terminal emulation.

Table D.10: VT52 Encoding

VT52 Keyboard	PC Character Sequence	VT52 Keyboard Byte Sequence
Delete	Delete	0x7F
Up Arrow	Up Arrow	Esc A
Down Arrow	Down Arrow	Esc B
Right Arrow	Right Arrow	Esc C
Left Arrow	Left Arrow	Esc D
Shift-F1	PF1	Esc P
Shift-F2	PF2	Esc Q
Shift-F3	PF3	Esc R
Shift-F4	PF4	Esc S

Table D.11 lists the decoding for VT52 terminal emulation.

Table D.11: VT52 Decoding

VT52 Keyboard Function	VT52 Keyboard Byte Sequence
Cursor Up	Esc A
Cursor Down	Esc B
Cursor Right	Esc C
Cursor Left	Esc D
Cursor Home	Esc H
Reverse Linefeed	Esc I
Erase to end of screen	Esc J
Erase to end of line	Esc K

Table D.12 lists the VT52 and ANSI auxiliary keypad definitions. Encoding of each listed keypad key is supported; decoding is not applicable.

Table D.12: VT52 ANSI Mode Auxiliary Keypad Definitions

Keys	Keypad Numeric Code	VT52 Keypad	ANSI Keyboard
0	0	Esc ? p	Esc O p
1	1	Esc ? q	Esc O q
2	2	Esc ? r	Esc O r
3	3	Esc ? s	Esc O s
4	4	Esc ? t	Esc O t
5	5	Esc ? u	Esc O u
6	6	Esc ? v	Esc O v
7	7	Esc ? w	Esc O w
8	8	Esc ? x	Esc O x
9	9	Esc ? y	Esc O y
- (dash)	- (dash)	Esc ? m	Esc O m
, (comma)	, (comma)	Esc ? l	Esc O l
. (period)	. (period)	Esc ? n	Esc O n
Enter	Same as Return key	Esc ? m	Esc O m

VT320 terminal emulation

Table D.13 lists the keystroke mapping (encoding) for VT320 terminal emulation.

Table D.13: VT320 Encoding

VT320 Keyboard	PC Character Sequence	VT320 Keyboard Byte Sequence
Escape Key (Esc)	Esc	0x1B
F1	F1	Esc O P
F2	F2	Esc O Q
F3	F3	Esc O R
F4	F4	Esc O S
F6	F6	Esc [1 7 ~

Table D.13: VT320 Encoding (Continued)

VT320 Keyboard	PC Character Sequence	VT320 Keyboard Byte Sequence
F7	F7	Esc [1 8 ~
F8	F8	Esc [1 9 ~
F9	F9	Esc [2 0 ~
F10	F10	Esc [2 1 ~
F11	F11	Esc [2 3 ~
F12	F12	Esc [2 4 ~
F13	Ctrl - F5	Esc [2 5 ~
F14	Ctrl - F6	Esc [2 6 ~
F15	Ctrl - F7	Esc [2 8 ~
F16	Ctrl - F8	Esc [2 9 ~
F17	Ctrl - F9	Esc [3 1 ~
F18	Ctrl - F10	Esc [3 2 ~
F19	Ctrl - F11	Esc [3 3 ~
F20	Ctrl - F12	Esc [3 4 ~
Insert	Insert	Esc [1 ~
Home	Home	Esc [2 ~
Delete	Delete	Hex 7 F
End	End	Esc [5 ~
Up Arrow	Up Arrow	Esc [A
Down Arrow	Down Arrow	Esc [B
Left Arrow	Left Arrow	Esc [D
Right Arrow	Right Arrow	Esc [C

Table D.14 lists the decoding for VT320 terminal emulation.

Table D.14: VT320 Decoding

VT320 Keyboard Function	VT320 Keyboard Byte Sequence
Index	Esc D

Table D.14: VT320 Decoding (Continued)

VT320 Keyboard Function	VT320 Keyboard Byte Sequence
New Line	Esc E
Reverse Index	Esc M
Escape O	Esc O
Save cursor and attributes	Esc 7
Restore cursor and attributes	Esc 8
Up Arrow	Esc [A
Down Arrow	Esc [B
Right Arrow	Esc [C
Left Arrow	Esc [D
Set cursor to home position	Esc [H
Set cursor to home position	Esc [f
Character Attributes	Esc [m
Erase from cursor to end of line	Esc [K
Erase from cursor to end of screen	Esc [J
Programmable LEDs	Esc [q
What are You?	Esc [c
Set Mode	Esc [?
Delete 1 Character	Esc [P
Insert 1 Line	Esc [L
Delete 1 Line	Esc [M
Up Arrow	Esc O A
Down Arrow	Esc O B
Right Arrow	Esc O C
Left Arrow	Esc O D
Fill Screen with Es	Esc # 8
Up Arrow amount specified by Pn	Esc [Pn A
Down Arrow amount specified by Pn	Esc [Pn B

Table D.14: VT320 Decoding (Continued)

VT320 Keyboard Function	VT320 Keyboard Byte Sequence
Right Arrow amount specified by Pn	Esc [Pn C
Left Down Arrow amount specified by Pn	Esc [Pn D
Erase parts of current line	Esc [Pn K
Erase parts of current screen	Esc [Pn J
Direct Cursor Addressing	Esc [Pn H
Direct Cursor Addressing	Esc [Pn f
Programmable LEDs	Esc [Pn q
Scrolling Region	Esc [Pn r
Clear tabs	Esc [Pn g
Device status report	Esc [Pn n
What are you?	Esc [Pn c
Sat Mode	Esc [Pn h
Delete Pn Characters	Esc [Pn P
Insert Pn Lines	Esc [Pn L
Delete Pn Lines	Esc [Pn M
Insert Character	Esc [Pn @
Erase Pn Characters	Esc [Pn X

Appendix E: Regaining Access to the DSView Software

Access to a DSView software system may be lost due to reasons such as:

- Being locked out by the DSView management software
- Deleting the last DSView software administrator
- Forgetting the DSView software administrator password

To regain access to a DSView software system:

1. Contact Avocent Technical Support. You will be provided with the resetpassword.zip archive file.
2. Extract the resetpassword.zip archive file into the <DSView Installation Directory>\bin directory on the DSView software hub server using a third party product.
3. From the Control Panel, select *Administrative Tools - Services* and stop the Avocent DSView software service.
4. Open a terminal window, change directories to the <DSView Installation Directory>/bin directory and enter **resetpassword.bat**. A code successfully generated message will appear in the terminal window, along with a request code in the same format as the following:

   341D3DAD-E71A15B1-66D77BBD-E655BB6C

NOTE: Request codes are valid for only 4 hours.

5. Contact Avocent Technical Support and provide the generated request code.
6. Avocent Technical Support will provide you with a reset code.
7. In a terminal window, enter **resetpassword.bat <reset code>**. A *Message reset performed successfully* message will appear in the terminal window, along with the Administrator username and password for the DSView management software.
8. From the Control Panel, select *Administrative Tools - Services* and restart the Avocent DSView software service.
9. You may now log into the DSView management software.

Appendix F: Glossary

Access control

Access control refers to mechanisms and policies that restrict access to computer resources.

Active Directory

Active Directory is the directory service included with Microsoft Windows 2000 and later versions of Windows operating systems. It extends the features of previous Windows-based directory services and contains new features that ease the navigation and management of large amounts of information, which may generate savings for both administrators and end users. Active Directory is secure, distributed, partitioned and replicated. It is designed to work well in any size installation, from a single server with a few hundred objects to thousands of servers and millions of objects.

ADSAP (Avocent DS Authentication Protocol)

ADSAP is a protocol used for authentication and authorization of DS1800 digital switches, DSR switches, CPS serial over IP appliance and CCM console management appliance target device sessions in the DSView management software. This is an SSL based protocol that uses X.509 certificates.

AIDP (Avocent Install and Discover Protocol)

AIDP is a protocol used to install out-of-box appliances that do not have an IP address assigned and used to discover existing appliances that have an address assigned. This UDP-based protocol is not encrypted and only public information is passed over this link. AIDP uses UDP port 3211. Port 3211 is non-configurable.

Applet

An applet is a program written in the Java language that runs within a web browser.

ASMP (Avocent Secure Management Protocol)

ASMP is a protocol used to securely configure managed appliance settings. This TCP-based protocol uses an SSL encrypted communications link. AMSP uses TCP port 3211. Port 3211 is non-configurable.

Authentication server

An authentication server is a network device that provides authentication services.

Authentication

Authentication is the validation of user login information. Authentication is used to enforce selective permission to access resources or to perform an operation.

Authorization

Authorization is the process of granting or denying access to a resource. Most computer security systems are based on a two-step process. The first stage is authentication, which ensures that users are who they claim to be. The second stage is authorization, which allows the user access to various resources based on the user's identity.

AVSP (Avocent Video Session Protocol)

A protocol used to transfer keyboard, video and mouse information between a DS1800 digital switch or DSR switch and a remote Video Viewer. AVSP operates over SSL encrypted TCP links. TCP/IP ports 8192 and 2068 are used by default, but may be configured to different port numbers.

Browser session

A type of target device session in which the target device contains a web server. The DSView software client connects directly to the target device using a web browser. No DS1800 digital switches, DSI5100, CPS or CCM appliances or DSR switches are used for browser sessions.

Cascade device

A device that connects between a DS1800 digital switch, DSR switch, CPS appliance or CCM appliance and a target device, or connects to a DS1800 digital switch, DSR switch, CPS appliance or CCM appliance and is not, in itself, a target device. Examples of cascade devices include a cascade switch and an SPC power control device.

Cascade switch

A cascade switch is an analog KVM switch connected to a DS1800 digital switch or DSR switch port or DSRIQ module. A cascade switch expands the number of connections allowed on a DS1800 digital switch or DSR switch if the switch supports the cascade protocol.

CCM appliance

A CCM console management appliance is an Avocent managed appliance that provides a Telnet server and an SSH server for accessing serially attached devices over a standard TCP/IP connection. Model numbers include the CCM850, CCM1650 and CCM4850 appliances.

Certificate authentication

Certificate authentication is the process of authenticating with a digital certificate.

CPS appliance

A CPS serial over IP network appliance is an Avocent managed appliance that provides a Telnet server and an SSH server for accessing serially attached devices over a standard TCP/IP connection. Model numbers include the CPS810 and CPS1610 appliances.

Database replication

Database replication is the process of distributing and keeping in sync the same database to all DSView software servers in a DSView software system. Database replication ensures that all database changes made at the hub server or spoke servers are replicated to all DSView software servers in the DSView software system.

The DSView management software versions of the spoke server and hub server must match in order to register the spoke server. For example, you may not register a spoke server running DSView software version 3.0 with a hub server running DSView software version 3.1.1.

DHCP (Dynamic Host Configuration Protocol)

DHCP is an Internet protocol used to automate the configuration of computers using TCP/IP. DHCP can be used to do the following:

- Assign IP addresses automatically

- Deliver TCP/IP stack configuration parameters, such as the subnet mask and default router
- Provide other configuration information, such as printer addresses

Digital Certificate

A digital certificate is an attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that users sending a message are who they claim to be, and to provide the receiver with the means to encode a reply.

An individual wishing to send an encrypted message applies for a digital certificate from a Certificate Authority (CA). The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or perhaps on the Internet.

The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply.

The most widely used standard for digital certificates is X.509.

DSR switch

The DSR switch is part of the Avocent digital KVM switch series of products that allows KVM signals to be transmitted over a standard TCP/IP connection.

DSRIQ module

A DSRIQ smart module uses CAT 5 cabling to attach a target device to a DS1800 digital switch or DSR switch. The DSRIQ module significantly reduces cable bulk in the rack and is well suited for high-density installations.

DSView management software

The DSView management software is an Avocent software component installed on a PC. The DSView management software provides the IP-based centralized services required for management of managed appliances and target devices, including centralized authentication, access control, logging events, monitoring, license management and so on. DSView software clients interact with the software using the DSView Explorer.

DSView software client

The DSView software client is a customer provided PC with an installed web browser. The web browser accesses the DSView software server and provides the user interface (that is, the DSView Explorer) for the DSView software system. The DSView Explorer enables users to access and administer the server, managed appliances and target devices.

DSView software client session

The DSView software client session is a single HTML session between the client web browser and the server. For each DSView software client session, the user must log into the DSView software server. Multiple DSView software client sessions can exist between a given DSView software client PC and the DSView software server. This occurs when the user launches another web browser window and connects to the same DSView software server.

A DSView software client session may contain multiple target device sessions.

DSView software hub server

A DSView software hub server is responsible for maintaining the master copy of the DSView software system database. Only one server in a DSView software system can be configured as the hub server. Spoke servers in a DSView software system perform database replication with the hub server. The DSView software hub server acts as the traffic cop for database replication between itself and all of the other servers in a DSView software system.

The DSView software hub server and a spoke server offer the same software functionality to a user. The distinction of hub or spoke only has to do with the database replication role the server plays and not with the software functionality the server offers to the user.

The DSView management software versions of the spoke server and hub server must match in order to register the spoke server. For example, you may not register a spoke server running DSView software version 3.0 with a DSView software hub server running DSView software version 3.1.1.

DSView software spoke server

A DSView software spoke server is responsible for initiating database replication with the hub server. A spoke server sends its database changes to the hub server and receives database changes from it.

The DSView software hub server and a spoke server offer the same software functionality to a user. The distinction of hub or spoke only has to do with the database replication role the server plays and not with the software functionality the server offers to the user.

The DSView management software versions of the spoke server and hub server must match in order to register the spoke server. For example, you may not register a spoke server running DSView software version 3.0 with a DSView software hub server running DSView software version 3.1.1.

DSView software server

A DSView software server is a customer provided PC on which the DSView management software is installed.

DSView software system

A DSView software system includes all the components required to provide DSView software functionality, including the DSView software server, DSView software client, managed appliances and target devices.

An SNMP manager and external authentication servers, which are optional components and outside the DSView software system, may also be added to provide additional functionality.

Encryption

Encryption is the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt the file. Unencrypted data is called plain text. Encrypted data is referred to as cipher text.

There are two main types of encryption: asymmetric (also called public-key encryption) and symmetric.

External authentication server

The external authentication server is an optional component(s) outside of the DSView software system that enables you to select an authentication method. The DSView software server brokers authentication requests (LDAP, RADIUS and so on).

Flash

Flash is a special type of EEPROM that can be erased and reprogrammed in blocks instead of one byte at a time. The BIOS and applications of many modern applications are stored on a Flash memory chip so that it may easily be updated (if necessary).

FRU (Field Replaceable Unit)

An FRU is a module or component which is typically completely replaced as part of a field service repair operation.

Graceful shutdown

A graceful shutdown is identical to a shutdown performed by selecting *Start - Shutdown* and then selecting *Shut down* in the Shut Down Window dialog box. In the DSView management software, a graceful shutdown may be performed on IPMI 1.5 target devices managed by a DSI5100 appliance.

Hotkey

A hotkey is a keystroke that may be assigned and used to cause a specific action or set of actions to occur within a user interface. By assigning the action(s), the keystroke's normal operation (for example, pressing **F1** to open help) is superseded.

HTML (Hypertext Markup Language)

HTML is a markup language used to create hypertext documents that are portable from one platform to another on the World Wide Web (WWW). HTML files are ASCII text files with embedded codes (markup tags) to indicate formatting and hypertext links. Web browsers interpret and display HTML documents.

HTTP (Hypertext Transfer Protocol)

HTTP is the underlying protocol by which WWW clients and servers communicate. HTTP is an application-level, generic, stateless, object-oriented protocol for distributed, collaborative, hypermedia information systems. A feature of HTTP is the typing and negotiation of data representation, allowing systems to be built independently of the data being transferred.

HTTPS (Secure Hypertext Transfer Protocol)

HTTPS is an extension to the HTTP protocol that supports sending data securely over the WWW.

Integrated windows authentication

Previously known as Windows NT Challenge/Response (NT/CR) or NT LAN Manager (NTLM), Integrated Windows Authentication is a secure form of web browser authentication

using either the Kerberos V5 authentication protocol or its own challenge/response authentication protocol.

This authentication method works best in an intranet environment where the types of web browsers that your network users access may be controlled. If you are already logged on to Windows, Integrated Windows Authentication uses your logon information for authentication, so it will not prompt for a username and password [known as Single Sign-On (SSO)].

Integrated Windows Authentication only works with Internet Explorer and does not work with an HTTP proxy. Integrated Windows Authentication must be explicitly enabled under the Advance Internet Options dialog box of Internet Explorer version 6.0 SP1 and above.

Java

Java is an environment for developing and deploying distributed, scalable, enterprise-level applications designed to run on networks, the Internet, and the WWW. The Java platform consists of a set of services, Application Program Interfaces (APIs) and protocols that provide functionality for developing multitiered, web-based applications.

KVM

KVM is an abbreviation of Keyboard, Video, Mouse.

KVM session

A KVM session is a type of target device session in which the target device contains a KVM connection (typically a server). KVM sessions are connected through a DS1800 digital switch or DSR switch. Tiered analog switches may also be part of the connection. A KVM Video Viewer connection exists between the DSView software client and the target device.

LDAP (Lightweight Directory Access Protocol)

LDAP is a set of protocols for accessing information directories. LDAP is based on standards contained in the X.500 standard, but is significantly simpler. Unlike X.500, LDAP supports TCP/IP, which is necessary for Internet access. Because LDAP is a simpler version of X.500, it is sometimes called X.500-lite.

Local port

The local port is the physical connection through which a DS1800 digital switch, DSR switch, CPS appliance or CCM appliance can be accessed without accessing a network connection.

For a DS1800 digital switch or DSR switch, the local port is typically the KVM connection at which a keyboard, mouse and monitor can be connected directly to the switch. An onscreen display may be invoked to control the DS1800 digital switch or DSR switch and access switched KVM ports.

For a CPS or CCM appliance, the local port is typically the serial connection at which a terminal can be connected directly to the appliance (CCM appliances have a dedicated console port). A command line interface (CLI) is used to control the appliance and access switched serial ports.

Managed appliance

Managed appliances include DS1800 digital switches, DSI5100 IPMI proxy appliances, DSR switches, CPS appliances, CCM appliances, EVR1500 environmental monitor and control appliances and generic appliances (such as routers).

MIB (Management Information Base)

MIB is a database of objects that can be monitored by a network management system (NMS). SNMP uses standardized MIB formats that allow any SNMP tools to monitor any device defined by an MIB.

NAT (Network Address Translation)

NAT is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located between the LAN and Internet makes all necessary IP address translations.

NAT serves three main purposes:

- Provides a type of firewall by hiding internal IP addresses.
- Enables a company to use more internal IP addresses. Since they're used internally only, there's no possibility of conflict with IP addresses used by other companies and organizations.
- Allows a company to combine multiple ISDN connections into a single Internet connection.

NAT device

A NAT device is a network address translation (NAT) device enables the use of more internal IP addresses than the number that are assigned. A NAT device provides IP addresses that are not exposed outside of the device. The DSView management software will not support network configuration where the DSView software server and CPS appliances, CCM appliances, DS1800 digital switches or DSR switches are separated by a NAT device.

Negative hysteresis

Negative hysteresis is the unsigned number of counts added to the raw threshold value, which creates the re-arm point for all sensor thresholds that are less than zero (0). A negative hysteresis value of 0 indicates that any thresholds less than zero do not contain hysteresis.

OSCAR interface

The OSCAR interface is a tool that is built in to Avocent appliances and allows a user connected to the local KVM port to display and change settings in a DS1800 digital switch or DSR switch. The OSCAR interface also allows a local user to connect to target devices.

PPP (Point to Point Protocol)

PPP is a set of industry-standard framing and authentication protocols included with Windows NT Remote Access Service to ensure interoperability with third party remote access software. PPP negotiates configuration parameters for multiple layers of the OSI (Open Systems Interconnection) model.

Positive hysteresis

Positive hysteresis is the unsigned number of counts subtracted from the raw threshold value, which creates the re-arm point for all sensor thresholds that are greater than zero (0). A positive hysteresis value of 0 indicates that any thresholds greater than zero do not contain hysteresis.

SDR repository device

An SDR repository device is the logical management device that provides a sensor data records (SDR) system interface, which in turn, provides a set of SDR storage and retrieval commands.

Serial session

A serial session is a type of target device session in which the target device contains a serial connection (typically a Linux server TTY port or a router) and is connected through a CPS or CCM appliance. A Telnet Viewer connection exists between the DSView software client and the CPS or CCM appliance. The appliance converts the Telnet information to serial information.

Server

A server is a computer or device on a network that manages network resources. For example:

- A file server is a computer and storage device dedicated to storing files. Any user on the network can store files on the server.
- A print server is a computer that manages one or more printers.
- A network server is a computer that manages network traffic.
- A database server is a computer system that processes database queries.

Servers are often dedicated, meaning that they perform no other tasks besides their server tasks. However, on multiprocessing operating systems, a single computer can execute several programs at once. In this case, a server may refer to the program that is managing resources rather than the entire computer.

Session

When used alone, a session refers to a target device session. See the definition of a target device session for details.

Site

A site is a location that contains a managed appliance, DSView software server or both.

SNMP (Simple Network Management Protocol)

SNMP is a set of protocols for managing complex networks. SNMP works by sending messages to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in MIBs and return this data to the SNMP requesters.

SNMP manager

The SNMP manager is an optional component (outside of the DSView software system) that enables the monitoring of many cross-platform devices using SNMP information. SNMP managers are also called network management systems (NMS).

SPC power control device

The SPC power control device is an Avocent cascade device that allows the remote controlling of target device power using a serial connection.

SSL (Secure Sockets Layer)

SSL is a protocol that supplies secure data communication through data encryption and decryption. SSL enables private communications over networks by using a combination of public key cryptography and bulk data encryption.

Target device

A target device includes a wide range of data center components such as servers and routers that an administrator is able to virtually manage through the DSView management software.

Target device session

A target device session is a connection through a KVM, serial, Telnet or web browser. Target device sessions do not include power management functionality.

TCP/IP (Transmission Control Protocol)

TCP is one of the main protocols in TCP/IP networks. The IP protocol deals only with packets. TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and that packets will be delivered in the same order in which they were sent.

Telnet session

A Telnet session is a type of target device session in which the target device supports Telnet and the DSView software client connects directly to the target device using Telnet.

Telnet Viewer

This applet is a software component that provides the user interface needed to display a remote target device through serial over IP sessions.

Tiered switch

A tiered switch is also known as a cascade switch. See the definition of cascade switch.

Unit

Unit is a generic term that refers to either a target device or a managed appliance. For example, the Unit List may contain both target devices and managed appliances.

UDP (User Datagram Protocol)

UDP is a connectionless protocol that runs on top of IP networks like TCP. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. UDP is primarily used for broadcasting messages over a network.

Video Viewer

The Video Viewer is a software component that provides the user interface needed to display a remote target device through KVM over IP sessions.

VPN (Virtual Private Network)

VPN is a means of implementing a private network on a public network such as the Internet. By encrypting data and assigning addresses, the impression is given to networks at each end of the VPN that they are connected by a private physical network instead of across a public network.

(WAN) Wide Area Network

WAN typically refers to a network that is distributed at multiple sites and connected by a relatively slow link between the sites. The WAN is frequently implemented using a VPN on the Internet.

(WAS) Web Application Server

WAS is software that runs on a server that is capable of executing web applications. The WAS software typically contains or works with a web (HTTP) server.

(Webapp) Web Application

Webapps are groups of server-side Web resources that make up an interactive online application. The web resources include Java servlets, JavaServer Pages™ (JSPs), static documents (such as HTML documents), and applets that can be deployed in a DSView software client web browser. Web applications must run in the context of a web application server such as the DSView software server.

Web server

A web server is a computer equipped with server software to respond to HTTP requests, such as requests from a web browser. A web server uses the HTTP protocol to communicate with clients on a TCP/IP network.

X.509

X.509 is the most widely used standard for defining digital certificates. X.509 is an International Telecommunications Union (ITU) recommendation, which means that the standard has not yet been officially defined or approved. As a result, companies have implemented the standard in different ways. For example, both Netscape and Microsoft use X.509 certificates to implement SSL in their web servers and web browsers. However, an X.509 certificate generated by Netscape may not be readable by Microsoft products, and vice versa.

INDEX

A

Access
about target device access rights 104
access control events 281
changing unit access rights 102
displaying user access rights to a managed appliance 163
displaying user access rights to a target device 162
mode (virtual media) 125
regaining access to DSView software 327
types 85
Active Directory authentication service
adding a service 59
changing service settings 67
changing user browsing settings 69
group naming 164
removing 73
ActiveX control
about 28
downloading using Windows (except XP) 28
downloading using Windows (XP only) 29
Appliances. See *Managed appliances*
Authentication services
about 58
adding Active Directory external services 59
adding LDAP external services 62
adding RADIUS external services 63
adding TACACS+ external services 64
adding Windows NT external services 61
changing Active Directory external service settings 67
changing Active Directory external service user browsing settings 69
changing internal authentication service account policies 65
changing internal authentication service custom field labels 66
changing LDAP external service connections 69
changing LDAP external service group schema settings 71
changing LDAP external service user browsing settings 71
changing LDAP external service user schema settings 71
changing RADIUS external service settings 72
changing TACACS+ external service settings 72
changing the IP addresses 107
changing Windows NT external service connections 66
changing Windows NT external service user browsing settings 67
events 279
group naming in external services 164
ports used 298
removing 73
specifying for a user-defined user group 165
specifying in a user account 153
supported services 58
validating user accounts on an external server using the Add Task Wizard 269

B

Backup and restore
manually using a command line 56
manually using the backup and restore utility 57
using the Add Task Wizard 259
BMCs. See *DSI5100 appliances*
Browsers

actions before opening a client session 45
supported for client 45

C

Cascade switches
displaying port settings 113
supported 5
CCM appliances
about 4
TCP ports used 294
See also *Managed Appliances*
Certificates
about 31
changing a certificate associated with a user 21, 156
correcting security alerts 26
creating a CSR 51
updating a spoke server certificate on the hub server 76
updating on a server 51
updating the hub server certificate on a spoke server 77
Color
changing color depth in Video Viewer windows 181
changing for the DSView Explorer 19
changing in Telnet Viewer window 211
changing when reviewing Telnet Viewer session data 217
Colors
displaying gauges in IPMI Viewer window 232
Compaq iLO embedded units
about 87
accessing 9, 85
adding 91
changing credentials 98
session considerations 88
supported versions 5
Connections
adding a target device connection 134
deleting a target device connection 135
display format 132
displaying current Video Viewer users 199
displaying information about 134
renaming a managed appliance connection 134
CPS appliances
about 4
TCP ports used 294
See also *Managed appliances*
Custom fields
associated a label with a unit 145
changing for a unit 100
changing for a user account 161
changing for user accounts that use internal authentication 66
defining 144
example 145
managing units by 144
Customize link
for Active Sessions window 130
for Appliance Access Rights window 162
for Appliance BMC Ports window 228
for Appliance Firmware Files window 272
for Appliance Local User Accounts window 127
for Appliance Serial Ports window 117
for Devices Attached to Appliance window 114
for Email Notifications window 286
for IPMI Discrete Sensors window 236
for IPMI Numeric Sensors window 238
for SPC Sockets window 115
for System Event Log window (DSI5100 appliances) 240
for Target Device Access Rights window 162
for Target Device Connections window 133
for Tasks window 256

for the Appliance Sessions window 121
for Unit Access Rights windows 168
for Unit views windows 84
for Units in Group window 143
for Units views windows 87
for User Accounts window 151
for User Groups windows 163
using 15

D

Departments 138
DRAC 4 embedded units
about 87
accessing 9, 85
adding 91
changing credentials 98
session considerations 88
supported versions 5
DS1800 digital switches
about 4
TCP ports used 292
See also *Managed appliances*
DSI5100 appliances
about 5
adding BMCs 227
changing BMC credentials 229
changing BMCs 227
changing identity settings 229
deleting BMCs 229
displaying FRU information 235
displaying IPMI 1.5 target device discrete sensor information 236
displaying IPMI 1.5 target device numeric sensor information 237
displaying IPMI target device BMC information 234
displaying LAN configuration information 235
displaying sensor information by selecting an IPMI target device 233
displaying sensor information using the IPMI Viewer 230
displaying the BMC system log and events 239
launching an IPMI Viewer session 230
sending an IPMI chassis control command to target devices using the Add Task Wizard 267
TCP ports used 299
See also *Managed appliances*
DSR Remote Operations software
about 301
displaying switch version information 309
exiting 310
icons - power view 305
icons - servers view 304
installing 43
managing servers 307
managing SPC device sockets 308
operating systems supported 43
power view 304
prerequisite actions 306
rebooting a switch 307
servers view 303
using 306
version view 305
window features 302
DSR switches
about 4
TCP ports used 292
See also *Managed appliances*
DSRIQ modules
deleting offline 112
displaying information 111
required for virtual media 201
upgrading 112
DSView 2.x software
importing databases into the DSView software

system 247
migrating units to DSView 3 software compatible units 264
DSView Explorer
bookmarking a window 17
changing the color scheme 19
changing user options 19
customizing information in a window 15
displaying pages 16
filtering information in a window 13
Internet Explorer configuration 26
printing a window 17
refreshing a window 17
saving information in a window 15
sorting information in a window 13
using keyboard commands 17
using the side navigation bar 12
window areas 8

E

Email
changing event log email notifications 287
configuring event log notifications 285
deleting event log notifications 287
specifying properties 55
testing event log notifications 288
Embedded units
about 87
accessing 9, 85
adding 91
changing access rights 102
changing credentials 98
session considerations 88
supported versions 5
Encryption
specifying for KVM sessions 124
specifying for virtual media sessions 202
specifying level for virtual media sessions 125
Event logs
about 275
access control events 281
appliance events 277
authentication events 279
changing email notifications 287
configuring email notifications 285
creating an event log .csv file 288
deleting email notifications 287
deleting events 284
displaying 281
displaying event details 284
displaying using a date filter 283
enabling/disabling events 284
exporting using the Add Task Wizard 262
icons in top navigation bar 283
retaining 285
session events 281
severity icons 276
severity levels 281
system events 278
task events 280
testing email notifications 288
unit events 279
unit status events 281
user and user group events 279
using the event log tool 288
Events
access control 281
appliance 277
authentication 279
session 281
system 278
task 280
unit 279
unit status 281

user and user group 279
EVR1500 environmental monitors
about 5
adding 94
changing network properties 102

F

Features and benefits 1
Firewalls 32, 292
Firmware
adding a firmware file 272
deleting 273
displaying appliance version information 111
displaying information about 272
updating the firmware of an appliance type using the Add Task Wizard 268
upgrading 252
upgrading DSRIQ modules 112

G

Generic appliances
about 5
adding 94
changing network properties 102
TCP ports used 296
Glossary 328
Groups
departments 138
locations 140
sites 135
units 135, 141

H

Hub server
about 3
registering a hub server as a spoke server 75
replication 77
specifying role during configuration 42
updating a spoke server certificate on the hub server 76
updting the hub server certificate on a spoke server 77

I

IBM ASM RSA II embedded units
about 87
accessing 9, 85
adding 91
changing credentials 98
session considerations 88
supported versions 5
Icons
DSR Remote Operations software - power view 305
DSR Remote Operations software - servers view 304
event log (top navigation bar) 283
severity of event log entries 276
spoke server status 74
task status 256
unit status 85
Installation
configuring the DSView software 41
hub server minimum requirements 38
installing the DSR Remote Operations software 43
installing the DSView software 38
minimum requirements for client 45
opening a client session 46
required tasks before installation 37
uninstalling 46
upgrading the DSView software 43
Integrated Windows Authentication 32, 54
Internal authentication service
changing account policies 65

changing custom field labels 66
Internet Explorer
ActiveX controls 28
adding a hub server to the Trust Sites list 30
changing security zone restrictions 30
configuring 26
correcting certificate security alerts 26
correcting serial session security alerts 27
specifying advanced Internet options 31
specifying security zones 29

J

Java installation 47

L

LDAP authentication service
adding 62
changing connections 69
changing group schema settings 71
changing user browsing settings 71
changing user schema settings 71
group naming 164
removing 73
Licenses
about 79
adding a new license key 80
displaying license information 79
displaying license key information 79
specifying a license key during configuration 42
Local accounts
adding 127
assigning target device access rights 129
changing access rights 102
changing settings 128
deleting 128
displaying information about 127
Locations 140
Logging. See *Telnet Viewer*

M

Macros. See *Exit macros, Macros (Telnet Viewer)* and *Macros (Video Viewer)*
Macros (Telnet Viewer)
about 217
creating 217
creating a macro group 219
deleting 219
deleting a macro group 220
editing 218
editing a macro group 220
enabling a macro group for use during a session 220
sending 219
Macros (Video Viewer)
about 192
adding/deleting macros in an existing macro group 196
changing the group to be displayed 198
copying 195
copying a macro group 198
creating a macro group 195
creating and editing 193
deleting 194
deleting a macro group 197
displaying a macro group 199
renaming a macro group 197
sending 193
Managed appliances
adding a firmware file 272
adding a generic appliance 94
adding a single appliance 89
adding an appliance from a range of IP addresses 93
adding an EVR1500 environmental monitor 94
changing an appliance name from the Unit

Overview window 97
changing local account settings 127
changing network properties 101
changing network settings 106
changing NFS settings (CCM appliances) 107
changing NTP settings (CCM appliances) 108
changing session settings 121
changing SNMP settings 109
configuring network settings 93
deleting firmware 273
displaying firmware information 272
displaying in Appliances window 81
displaying the Appliance Firmware Files window 272
displaying user access rights 163
displaying version information 111
enabling/disabling secure mode 90, 94
events 277
rebooting 251
restoring a configuration 254
restoring a user database 255
resynchronizing 252
saving a configuration 253
saving a user database 254
updating the firmware of an appliance type using the Add Task Wizard 268
upgrading firmware 252
See also *SNMP*
Migration
AVWorks software CCM appliances to DSView software compatible units 265
DSView 2.x software units to DSView 3 software compatible units 264
Mouse settings
aligning in the Video Viewer 187
required before software installation 37
See also *Video Viewer* 37

N

NAT devices 34
NEC IPF
changing credentials 98
NEC IPF embedded units
about 87
accessing 9, 85
adding 91
session considerations 88
supported versions 5
Network settings for managed appliances 93
NFS settings and status (CCM appliances) 107
NTP status and settings (CCM appliances) 108

O

Operating systems
supported for client 45
supported for DSR Remote Operations software 43
supported for hub server 38
OSCAR interface
changing authentication setting 113

P

Password
changing 20
changing for a user 158
enabling/disabling expiration and change restrictions 158
regaining access when software administrator password is lost 327
resetting in a user account 155
Ports
changing CLI/console port settings for a CPS or CCM appliance 119
changing communications properties of a serial port (CCM and CPS appliances) 118
changing local OSCAR interface authentication

settings 113
changing modem port settings 114
changing PPP settings (CPS and CCM appliances) 120
changing PPP setttings (CPS and CCM appliances) 120
changing serial port general properties 117
displaying cascade switch port settings 113
TCP 292
Preemption
about 24
changing in a user account 159
considerations in virtual media sessions 201
preempting a Video Viewer session 173
specifying for user-defined user group 166
specifying level in user account 154
Profile
about 19
changing the certificate associated with a user 21
changing the color scheme 19
changing user options 19
enabling a third party Telnet application 20
specifying a user SSH key 22
Properties
about hub server properties 49
changing contact properties 100
changing hub server network properties 50
changing spoke server network properties 76
changing unit identity properties 99
changing unit location properties 100
changing unit note properties 101
configuring unit status polling 55
creating a CSR 51
displaying server properties 50
specifying a proxy server 53
specifying client session information 54
specifying email notification information 55
specifying trap destinations 54
updating a certificate on a server 51
Proxy server
about 49
specifying 53

R

RADIUS authentication service
adding 63
changing settings 72
removing 73
Remote operations. See *DSR Remote Operations software*
Replication 77
Requirements
client 45
hub server 38
Video Viewer 172
virtual media 201

S

Scan mode
about 187
changing the thumbnail size 190
disabling a device thumbnail in the scan sequence 190
enabling a device thumbnail in the scan sequence 190
exiting the Thumbnail Viewer 191
launching a session to a device 190
pausing and restarting a scan sequence 190
setting scan preferences 190
Thumbnail Viewer features 188
See also *Video Viewer*
Secure mode 90, 94
Security zones
adding a hub server to the Trusted Sites list 30
changing restrictions 30

specifying 29
Servers
about properties 49
backing up and restoring a hub 55
changing hub server network properties 50
configuring unit status polling 55
creating a CSR 51
deleting a spoke server 77
displaying properties 50
managing authentication services 58
managing spoke servers 73
registering a hub server as a spoke server 75
replication 77
specifying a proxy server 53
specifying client session information 54
specifying email notification properties 55
specifying role (hub or spoke) during configuration 42
specifying trap destinations 54
updating a certificate 51, 76
See also *Authentication services* , *Hub server* and *Spoke servers* 49
Sessions
access methods 85
before opening a client session 45
changing CPS or CCM appliance session settings 123
changing KVM session settings 124
changing virtual media session settings 124
closing a session 47
closing a Telnet Viewer session 226
closing a virtual media session 204
correcting serial session security alerts 27
customizing Telnet Viewer session properties 212
customizing the Active Sessions window 130
disconnecting an active session 131
displaying active session information 131
displaying appliance session information 123
events 281
launching a device session from the Thumbnail Viewer 190
managing active 129
opening a client session 46
opening a Telnet Viewer session 210
opening a virtual media session 203
removing an active session from display in the Active Sessions window 131
sharing (CPS and CCM appliances) 123
sharing (Video Viewer) 173
specifying client information 54
specifying Video Viewer session settings 177
Video Viewer session time-out 174
Sites 135
SNMP
changing settings 109
enabling/disabling 109
enabling/disabling SNMP manager settings 110
enabling/disabling traps 111
enabling/disabling traps using the Add Task Wizard 260
ports used 298
specifying destination settings 110
specifying DSView software trap destinations 54
specifying SNMP community settings 110
SPC devices
about 6
changing port settings 115
changing socket settings 116
displaying in Topology view 82
managing sockets using DSR Remote Operations software 308
power controlling from a Telnet Viewer session 225
power controlling from the SPC Devices

Attached to Appliance window 116
power controlling from the Unit Overview window 97
power controlling from the Video Viewer 199
power controlling using the Add Task wizard 261
Spoke servers
about 3
adding 75
changing network properties 76
deleting 77
displaying a list 74
managing 73
registering a hub server as a spoke server 75
replication 77
specifying role during configuration 42
status icons 74
updating a spoke server certificate on the hub server 76
updating the hub server certificate on a spoke server 77
SSH key
specifying in a profile 22
specifying in a user account 157
Status
configuring unit status polling 55
spoke server status icons 74
task status icons 256
unit status events 281
unit status icons 85
unit status IDs 84

T

TACACS+ authentication service
adding 64
changing settings 72
removing 73
Target devices
about 6
access rights displays 104, 162, 168
accessing 9, 85
adding 6, 95
adding a connection 134
allowing/preventing those with default names from being added 90, 94
allowing/preventing those with same name to be merged 90, 94
assigning access to a local account 129
changing access rights 104
changing network properties 101
changing Unit Overview information 96
configuring device settings 95
deleting a connection 135
displaying in Target Devices window 81
displaying in Topology view 82
displaying user access rights 162
merging 246
working with IPMI 1.5 target devices 227
See also *DSI5100 appliances*
See also *SPC devices*
Tasks
adding 256
adding tasks using the Add Task wizard 259
changing a task's schedule 271
changing task properties 271
deleting 271
displaying results 270
events 280
managing 255
running manually 270
specifying when to run tasks 257
status icons 256
TCP ports 292
Technical support 291
Telnet

enabling/disabling use of a third party application 20
See also *Telnet Viewer*
Telnet Viewer
about 207
changing the cursor 211
changing the linefeed settings 214
changing the terminal emulation mode 212
changing the terminal window size 212
changing window and background colors 211
changing window and background colors when reviewing session data 217
closing a session 226
copying, pasting and printing session data 223
customizing session properties 212
enabling/disabling 7-bit ASCII 215
enabling/disabling automatic login 216
enabling/disabling autoscaling 212
enabling/disabling line wrap 214
enabling/disabling local echo 215
enabling/disabling the exit warning prompt 212
Java requirements 47
logging 221
login scripts 215
macros 217
opening a session 210
power controlling SPC devices 225
reviewing session data 216
security features 210
terminal emulation 311
window features 208
Thumbnail Viewer. See *Scan mode*
Tools
displaying the Units Tools window 243, 251
exporting an event log 262
exporting unit rights 245
exporting units 243
firmware management 272
importing DSView 2.x software databases 247
merging target devices 246
rebooting a managed appliance 251
restoring a managed appliance configuration 254
restoring a user database 255
resynchronizing managed appliances 252
saving a managed appliance configuration 253
saving a managed appliance user database 254
upgrading firmware 252
Events
See also *Event logs*
Groups
See also *User Groups*
Topology view 82
about 82
displaying units and SPC devices 82
Traps. See *SNMP*

U

Units
about Units views 81
accessing 85
accessing the managed appliance tools 251
adding 88
changing managed appliance settings 106
changing properties 99
changing unit access rights 102
configuring unit status polling 55
customizing Units views windows 84
displaying information 81
embedded. See *Embedded units*
events 279
exporting 243
exporting unit rights 245
grouping by department 138
grouping by location 140

grouping by unit group 141
grouping units by sites 135
groups 135
hiding a unit 83
information in Overview window 95
managing by custom fields 144
managing connections 132
managing port settings 111
showing and hiding 83
showing hidden units 84
status icons 85
status IDs 84
tools 243
unit groups 141
unit status events 281
views 81
See also *Tools*, *Managed appliances*, *Target devices* and *SPC devices*

User accounts
adding a user 153
changing a password 20, 158
changing a user's group membership 158
changing custom fields 161
changing the certificate associated with a user 156
changing the preemption level 159
changing the user name 156
changing unit access rights 102
deleting 155
displaying User Accounts window 151
events 279
resetting a password 155
specifying a user SSH key 157
specifying email contact 160
specifying password restrictions 158
specifying phone contact 160
specifying user address 159
unlocking 155
user options when using DSView Explorer 19
validating on an external authentication server using the Add Task Wizard 269
windows 149
See also *Local user accounts* and *User groups*

User groups
about 163
adding a user-defined group 164
assigning in user account 154
assigning or removing a member 167
built-in 22, 163
changing a user's membership 158
changing unit access rights 102
deleting a user-defined group 166
displaying access rights of a target device 168
displaying access rights of managed appliances 169
displaying and changing group properties 166
displaying built-in group properties 166
displaying or changing user-defined group properties 166
displaying User Groups windows 164
events 279
specifying a preemption level 166

V

Video noise compensation 124
Video Viewer
about 171
adding/removing macros or commands from the toolbar 178
adjusting color depth 181
adjusting mouse options 184
adjusting the view 179, 181
aligning the mouse 187
capturing a window 200
changing the window resolution 178

closing a session 200
connecting to an existing KVM session 173
displaying current users 199
enabling scaling types 180
enabling/disabling full screen mode 179
Java requirements 47
launching a KVM session 172
launching an exclusive KVM session 173
macros 192
minimum requirements 172
preempting connections 173
refreshing the screen 179
selecting the cursor type 185
session time-out 174
sharing connections 173
specifying a toolbar hide time 177
specifying scaling 186
specifying session settings 177
toggling activation of menu and toolbar 178
troubleshooting 205
using background refresh 180
using keyboard pass-through 191
using scan mode 187
using virtual media 200
window features 175
See also *Scan Mode*

Virtual media
access mode 125
changing session settings 124
changing unit access rights to allow virtual media sessions 105
closing a session 204
dialog box 202
displaying drive details 204
encryption level 202
locking to KVM session 125, 202
mapped drive access mode 202
mapping drives 203
opening a session 203
requirements 201
reserved sessions 201
resetting USB devices on the target device 204
session settings 202
sharing and preemption considerations 201
unmapping drives 204

VPNs 33
VT terminal emulation 311
VT100 terminal emulation 313
VT100+ terminal emulation 312
VT102 terminal emulation 312
VT220 terminal emulation 319
VT320 terminal emulation 323
VT52 terminal emulation 322

W

Window. See *DSView Explorer*
Windows NT authentication service
adding a service 61
changing connections 66
changing user browsing settings 67
removing 73

Wizards
Add Authentication Service
Active Directory 59
LDAP 62
RADIUS 63
TACACS+ 64
Windows NT 61
Add Email Notification 286
Add Firmware File 272
Add IPMI BMC 228
Add Local User Account 127
Add Target Device Connection 134
Add Task 256, 259
Add Unit 89, 93, 94, 95

Add Unit Group 142
Add User 153
Add User Group 165
Export Event Log 288
Export Unit Rights 245
Export Units 244
Import DSView 2.x Database 249
Merge Target Devices 246
Restore Appliance Configuration 254
Restore Appliance User Database 255
Resync Appliance 253
Save Appliance Configuration 254
Save Appliance User Database 255
Server Configuration 42
Update DSView Server Certificate 51

Avocent
The Power of Being There®

For Technical Support:
www.avocent.com/support

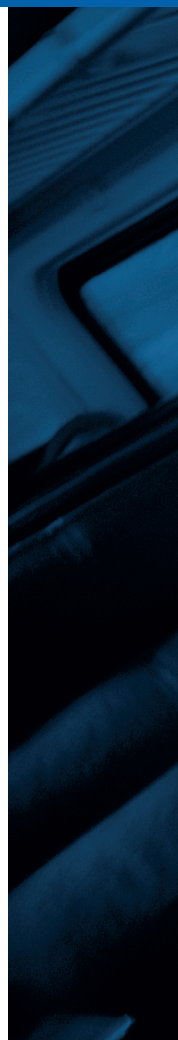
Avocent Corporation
4991 Corporate Drive
Huntsville, Alabama 35805-6201 USA
Tel: +1 256 430 4000
Fax: +1 256 430 4031

Avocent International Ltd.
Avocent House, Shannon Free Zone
Shannon, County Clare, Ireland
Tel: +353 61 715 292
Fax: +353 61 471 871

Avocent Asia Pacific
Singapore Branch Office
100 Tras Street, #15-01
Amara Corporate Tower
Singapore 079027
Tel: +656 227 3773
Fax: +656 223 9155

Avocent Germany
Gottlieb-Daimler-Straße 2-4
D-33803 Steinhagen
Germany
Tel: +49 5204 9134 0
Fax: +49 5204 9134 99

Avocent Canada
20 Mural Street, Unit 5
Richmond Hill, Ontario
L4B 1K3 Canada
Tel: +1 877 992 9239
Fax: +1 877 524 2985



590-395-501D